TRABALHO DE GRADUAÇÃO

ESTUDO E IMPLEMENTAÇÃO DE CONTROLADORES PARA SISTEMAS RFID

Débora Andrade Bastos

Flávia Marques da Silva

Brasília, dezembro de 2007

UNIVERSIDADE DE BRASÍLIA

FACULDADE DE TECNOLOGIA

UNIVERSIDADE DE BRASILIA
Faculdade de Tecnologia

TRABALHO DE GRADUAÇÃO

ESTUDO E IMPLEMENTAÇÃO DE CONTROLADORES PARA SISTEMAS RFID

Débora Andrade Bastos

Flávia Marques da Silva

Relatório submetido ao Departamento de Engenharia Elétrica como requisito parcial para obtenção do grau de Engenheiro Eletricista

Banca Examinadora

Prof. Dr. Antônio José Martins Soares, ENE/UnB ______________________
Orientador

Prof. Dr. Leonardo R.A.X. de Menezes, ENE/UnB ______________________
Examinador interno

Prof. Dr. Plínio Ricardo Ganime Alves, ENE/UnB ______________________
Examinador interno

Dedicatórias

Dedico este trabalho à todos que estiveram ao meu lado nos bons e nos maus momentos que passei durante o curso. Dedico também à Tabita que hoje está cuidando de mim lá do céu.

Flávia Marques da Silva

Mãe, você sempre foi fonte de inspiração, exemplo de força. Hoje desempenha também o papel de pai sem nenhum deslize. Seria impossível vencer sem você.

Débora Andrade Bastos

Agradecimentos

Agradeço a Deus por minha família, que me apóia sempre, compartilhando alegrias e tristezas. Agradeço ao grande mestre Martins. Agradeço aos amigos, tão verdadeiros, compreensivos e sempre presentes. Em especial à Flavinha, que além de amiga e confidente, é uma excelente companheira de trabalho. Também ao Alvinho pela amizade, companheirismo, compreensão, dedicação, carinho e amor. Finalmente, ao meu engenheiro modelo, anjo da guarda e pai, que em algum lugar do céu me guia, sussurrando palavras doces.

Débora Andrade Bastos

Agradeço primeiramente a Deus que me deu força e coragem para chegar ao fim deste curso. Ao meu professor e orientador Martins que tornou a produção desse trabalho extremamente motivante. Aos meus pais, que independentemente de qualquer coisa são meus alicerces. Ao meu irmão que me mostrou o que é se doar para alguém além de mostrar que é muito digno da minha admiração. À minha irmã que é um anjinho em minha vida. À minha dupla de trabalho e grande amiga Debinha, pessoa muito especial pra mim. Aos amigos de longa data e às pessoas maravilhosas que conheci nos últimos 5 anos de faculdade. À todos que me ajudam e me ajudaram nos momentos difíceis. Não sei como seria sem todos vocês!

Flávia Marques da Silva

RESUMO

Neste trabalho é realizado um estudo de controladores RFID (*Radiofrequency Identification* - Identificação por Radiofreqüência). Esses controladores são sistemas que realizam o gerenciamento das aplicações que utilizam a tecnologia em estudo. A partir da análise do funcionamento dos controladores estudados, propõe-se um sistema para utilização em uma aplicação específica, uma livraria. Como não há ambiente real de teste, o funcionamento do sistema proposto é simulado. Tal sistema é implementado na linguagem Java por ser a linguagem mais utilizada para desenvolvimento desse tipo de aplicação.

ABSTRACT

This project is a study about RFID (Radiofrequency Identification) controllers. These controllers are management systems of aplications based on this technology. From the analisis of the existing controllers, a system is developed fon an especific application, a bookstore. Since there is not a real RFID testing enviroment, the developed system is simulated in order to show its functions. This system is implemented using Java language because this language is the most common in this sort of application.

SUMÁRIO

LISTA DE FIGURAS

LISTA DE TABELAS

1 INTRODUÇÃO

Se hoje há tanta sofisticação na comunicação por radiofreqüência, boa parte é devida a sir Robert Alexander Watson-Watt, físico escocês responsável pela invenção, em 1935, dos sistemas de RADAR (*Radio Detection And Ranging*) usados durante a segunda guerra mundial. Na mesma época, foi desenvolvido o primeiro sistema ativo de identificação por radiofreqüência (RFID). Seu funcionamento era bem simples: foi colocado um transmissor em cada avião britânico; quando o mesmo recebia sinais das estações de radar no solo, era então transmitido um sinal de volta para identificar que o avião era amigo.

Em 23 de janeiro de 1973, Mario W. Cardullo, criou e requereu a patente para uma etiqueta ativa de RFID com uma memória regravável. Charles Walton, um empreendedor da Califórnia, recebeu a patente por um transponder passivo usado para destravar uma porta sem a utilização de uma chave. Um cartão com um transponder embutido comunicava com um leitor/receptor localizado perto da porta. Quando o receptor detectava um número de identificação válido armazenado na etiqueta RFID, a porta era destravada através de um mecanismo [1].

O governo dos Estados Unidos também tem voltado atenção para os sistemas RFID. Na década de 1970, o laboratório nacional de Los Alamos recebeu um pedido do departamento de energia para desenvolver um sistema para rastrear materiais nucleares. Um grupo de cientistas idealizou um projeto onde seria colocado um transponder em cada caminhão transportador, ao qual corresponderia uma identificação e, potencialmente, outro tipo de informação, como, por exemplo, a identificação do motorista.

No começo da década de 90, engenheiros da IBM desenvolveram e patentearam um sistema de RFID em UHF (*Ultra High Frequency*). Em UHF, o alcance de leitura é de aproximadamente 6 metros sobre condições boas e a transferência de dados ocorre em alta velocidade. Apesar de realizar testes com a rede de supermercados Wal-Mart, a IBM não chegou a comercializar essa tecnologia, mas em meados de 1990, vendeu a patente para a Intermec, um provedor de sistemas de código de barras. Após isso, o sistema de RFID da Intermec tem sido instalado em inúmeras aplicações diferentes, desde controle de estoques até criações de animais. No entanto, a tecnologia era muito cara comparada ao pequeno volume de vendas, e a tinha pouco interesse internacional.

A tecnologia RFID em UHF teve uma melhora na sua visibilidade em 1999, quando o Uniform Code Concil, o EAN internacional, a Procter Gamble e a Gillette se uniram e estabeleceram o Auto-ID Center, no Instituto de Tecnologia de Massachusetts. Desde então, os professores David Brock e Sanjay Sarma, têm realizado pesquisas para viabilizar a utilização de etiquetas de RFID de baixo custo em todos os produtos, a fim de rastreá-los. A idéia consiste em colocar apenas um número serial em cada etiqueta para manter o preço baixo (utilizando-se apenas de um microchip simples que armazenaria pouca informação). A informação associada ao número serial de cada etiqueta pode ser armazenada em qualquer banco de dados externo, acessível inclusive pela Internet [2].

O desafio de hoje é atender a demanda por sistemas rápidos que garantam confiabilidade, segurança e escalabilidade. O sistema RFID é uma implementação que evolui neste sentido, já que visa proporcionar um controle intenso dos objetos rastreados, algumas vezes até em tempo real. Um exemplo é o controle de estoque de uma empresa, permitido por sucessivas leituras das etiquetas identificadoras dos produtos. Um

portal de leitura delimita uma área e registra a movimentação do produto; a desmagnetização da etiqueta permite a saída do item da empresa, mas mantém os registros anteriores daquele produto. É possível também rastrear a fase de transporte de um produto ou de um lote fechado com vários produtos. Para isso, uma etiqueta é gravada e colada às mercadorias, contendo informações sobre a carga, tais como endereço para entrega, telefone, previsão de chegada, quantidade de produtos no lote, data de validade, especificações do lote, e várias outras informações. Durante a fase de transportes, o veículo monitora a carga e, por sua vez, é monitorado pela central via GPS. O destinatário, ao receber o lote, realiza a leitura da etiqueta, confirma as informações do pedido e confere os produtos. Caso tudo esteja correto, uma mensagem é enviada via internet para o remetente, avisando o *status* do recebimento do lote. Percebe-se que o RFID é uma tecnologia que se beneficia de tecnologias já existentes, como GPS e Internet, para garantir um ambiente seguro desde a fabricação do produto até a chegada ao usuário final.

A implementação de um sistema de controle tão eficaz como o sistema RFID, demanda rotinas e processamento das informações para reduzir o fluxo inadvertido e desnecessário dos dados. Processar todo o conteúdo proveniente do sistema causaria sobrecarga da rede e redução da velocidade de trabalho da ferramenta completa. Controladores RFID agregam, condensam, filtram e armazenam os dados provenientes das inúmeras leituras das etiquetas. Eles são compostos por instrumentos, como etiquetas ativas ou passsivas, leitores e pelo menos uma unidade central de processamento. Desta forma, todos os dados adquiridos pelo sistema RFID são interpretados inicialmente, processados de acordo com as configurações pré-definidas pelo usuário e somente as informações essenciais, como situações de risco ou exceções, serão processadas e então visualizadas pelo gerenciador do sistema.

Esse trabalho tem por objetivo a análise do contexto no qual RFID se insere, suas principais aplicações hoje existentes e os controladores mais utilizados comercialmente. A partir do estudo aprofundado desses controladores, deseja-se propor um software semelhante aos controladores apresentados, porém limitado às simulações, devido ao ambiente de desenvolvimento não possuir os equipamentos de hardware necessários para o desenvolvimento de uma solução fim a fim.

No capítulo 2 é feita uma revisão bibliográfica sobre o tema de estudo. Em seguida, o capítulo 3 descreve os principais controladores de fluxo utilizados por detentores da tecnologia RFID. O capítulo 4 introduz a metodologia empregada e o cenário de desenvolvimento de um software que atua como controlador RFID e também agrega funções comerciais. O manual de utilização do software proposto com estudo de caso é apresentado no capítulo 5, seguido das conclusões do projeto, apresentadas no capítulo 6.

2 SISTEMAS AUTO-ID

2.1 INTRODUÇÃO

Identificação por radiofreqüência (*Radio Frequency Identification* - RFID) é um termo genérico usado para descrever sistemas que transmitem a identidade (normalmente um número serial único) de um objeto ou pessoa. Para realizar essa identificação, é utilizado ondas de rádio. Existem ainda outras formas de identificação, agrupadas em uma categoria mais geral, constituída por tecnologias de identificação automática (*automatic identification*, aqui denominado Auto-ID), como pode ser visto na figura 2.1. Este capítulo tratará dos equipamentos que compõem os sistemas Auto-ID. O sistema RFID é um tipo de sistema Auto-ID. Ele será apresentado, junto a algumas aplicações possíveis para esse sistema. Os conceitos aqui apresentados são referenciados no livro RFID Handbook [3].

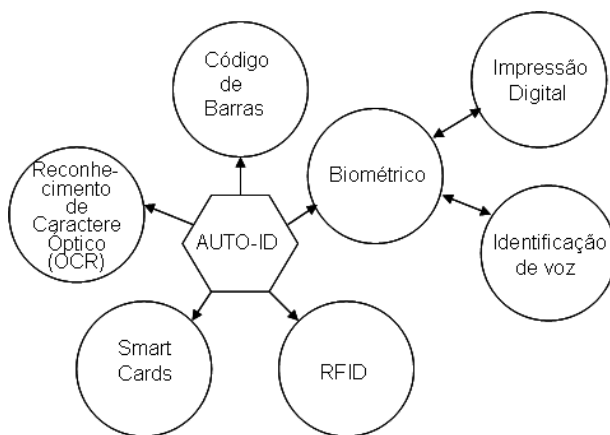



Figura 2.1: Sistemas Auto-ID.

2.2 SISTEMAS AUTO-ID

2.2.1 Código de Barras

O código de barras é um código binário composto por um arranjo de barras e espaços em paralelo. A seqüência de barras e espaços representa um código numérico ou alfanumérico. O código é lido por um scanner de laser pela diferença de reflexão do feixe do laser incidente nas barras (negras) e nos espaços (brancos). Apesar de os vários códigos de barras serem parecidos visualmente, eles são bastante diferentes no que diz respeito a layout. O mais utilizado é o código EAN (*European Article Number*) desenvolvido para atender a indústria alimentícia, em 1976.

O código EAN, composto por 13 dígitos, contém a identificação do país, a identificação da empresa, o número do produto e um dígito de checagem (DC). A figura 2.2 ilustra um exemplo do código EAN.

Identificador de País		Identificador da Companhia					Número do item do fabricante					DC
4	0	1	2	3	4	5	0	8	1	5	0	9
BRA		Empresa de Páscoa R. do Ouvidor, 200. Rio de Janeiro					Ovo de Páscoa 200 gr.					

Figura 2.2: Exemplo do Código de Barras na codificacão EAN.

2.2.2 Identificação de Voz

A identificação de voz é um dos métodos de identificação que utiliza procedimentos biométricos. No contexto dos sistemas de identificação, biometria é o termo geral utilizado para todos os procedimentos de identificação de pessoas por comparação de características físicas individuais e sem a possibilidade de cometimento de erro ou engano. Entre os procedimentos biométricos, estão a identificação de impressão digital e impressão da mão, identificação de voz e, menos comum, identificação de íris.

Os sistemas de identificação de voz fazem a verificação da voz do locutor. Nesse sistema, o usuário fala em um microfone que está conectado a um computador. O sinal de voz é convertido em sinal elétrico pelo microfone e, a seguir, em sinal digital pelo computador. O sinal digital é comparado por um software de identificação com sinais previamente gravados e armazenados no computador. Quando um padrão é encontrado entre a voz recebida e uma das vozes anteriormente gravadas, a identificação do locutor é concluída e uma ação é executada, como, por exemplo, a liberação de uma porta para sistemas de segurança de entrada em ambientes.

2.2.3 Impressão Digital

A identificação por impressão digital é um processo baseado na comparação dos sulcos da derme das pontas dos dedos. A impressão digital pode ser obtida não somente dos próprios dedos, mas também de objetos que um indivíduo possa ter tocado.

A identificação de pessoas utilizando impressão digital normalmente é utilizada para controle de acesso. A pessoa que deseja entrar em um ambiente com acesso controlado por identificação de impressão digital deve colocar a ponta do dedo em um leitor especial. O sistema calcula o padrão do dado registrado que ele acabou de ler e compara com os padrões de referência armazenados. Caso encontre um registro armazenado que se assemelhe com o dado recém lido, a identificação é feita e a entrada da pessoa no recinto pode ser ou não autorizada.

2.2.4 *Smart Cards*

Os *Smarts Cards* são sistemas eletrônicos de armazenamento de dados com a possibilidade de alguma capacidade computacional, para o caso de cartões microprocessados. Os *Smarts Cards* têm normalmente o formato de um cartão magnético, como os cartões de crédito. A diferença entre os Smarts Cards e as etiquetas RFID é o fato de os *Smarts Cards* necessitarem de ter contato físico (superfícies de contato) com o leitor para fazer uma conexão galvânica entre leitor e cartão. Os *Smarts Cards* são supridos de energia e relógio pelo leitor através das superfícies de contato. A transferência de dados entre cartão e leitor ocorre usando a interface serial bidirecional (porta de I/O).

Uma das grandes vantagens dos *Smarts Cards* é a proteção das informações contidas nos cartões contra acesso indesejável e manipulação indevida dos dados.

Existem dois tipos diferentes de *Smarts Cards* baseados em suas funcionalidades internas: o cartão de memória e o cartão microprocessado.

- Cartão de Memória

Cartões de memória normalmente utilizam como dispositivo de armazenamento a memória EEPROM (*Electrically Erasable Programmable Read-Only Memory* - Memória somente de Leitura Programável e Apagável Eletricamente). Nesses cartões, a forma de acesso à memória utiliza uma lógica seqüencial, o acesso é feito por meio de uma máquina de estados.

Esse tipo de cartão pode ter incorporado mecanismos de segurança, como algoritmos simples de segurança. Nesse sistema, a flexibilidade na aplicação é extremamente reduzida, visto que a memória EEPROM não permite troca de informações entre leitor e tag. Mas, em contrapartida, cartões de memória têm custos bastante reduzidos considerando-se a eficiência que os sistemas que utilizam essa tecnologia oferecem. Por essa razão, os sistemas utilizando cartões de memória são predominantemente utilizados em sistemas de consulta de preços, que são aplicações de larga escala. Os contatos galvânicos e a lógica interna dos cartões de memória estão ilustradas na figura 2.3.

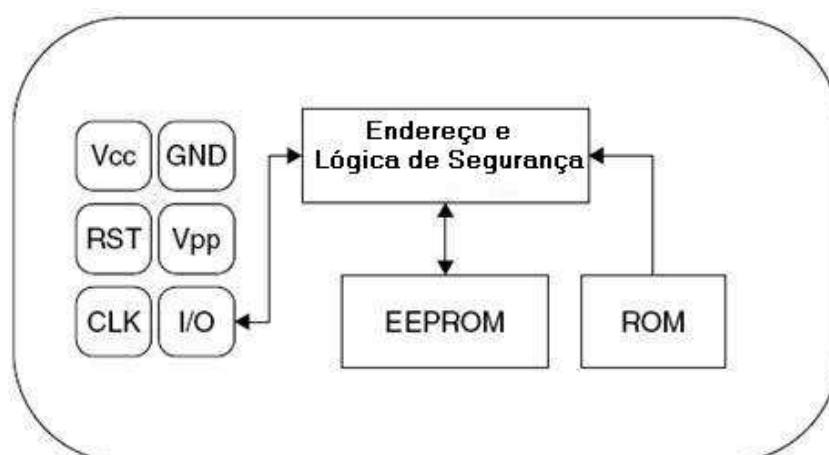



Figura 2.3: Lógica interna de um cartão de memória.

- Cartão Microprocessado

Cartões microprocessados contêm, como o próprio nome sugere, um microprocessador conectado a um segmento de memória (segmentos ROM, RAM e EEPROM).

A ROM (*Read-Only Memory* - Memória somente de leitura) é provida de um sistema operacional (programa principal) para programar o microprocessador e é inserido durante a fabricação do chip. O conteúdo da ROM é semelhante para todos os chips que são fabricados no mesmo lote. O sistema operacional não pode ser sobrescrito.

A EEPROM contém as informações da aplicação e o código relativo à aplicação. A leitura e a escrita nessa área de memória é controlada pelo sistema operacional.

A RAM (*Random Access Memory* - Memória de Acesso Aleatório) é a área de memória temporária do microprocessador. Os dados são armazenados na RAM somente enquanto ela está sendo suprida por uma fonte de alimentação. Quando a alimentação é retirada, os dados armazenados na RAM são perdidos definitivamente.

Cartões microprocessados são extremamente flexíveis. Em cartões mais modernos é possível a utilização de mais de uma aplicação integrada em um único cartão (cartão multi-aplicação).

A lógica interna de um cartão microprocessado pode ser vista na figura 2.4.

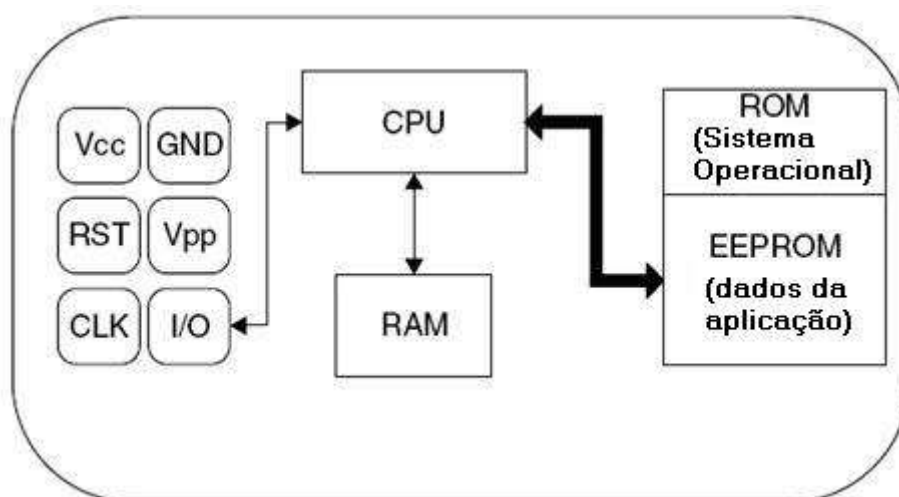



Figura 2.4: Lógica interna de um cartão microprocessado.

2.2.5 Sistemas RFID

Sistemas RFID são semelhantes aos Smart Cards descritos anteriormente. A principal diferença entre esses dois sistemas de identificação é que a alimentação do dispositivo RFID que contém as informações para a identificação, bem como a troca de informações entre esse dispositivo e o leitor, é realizada sem a utilização de contatos galvânicos. A alimentação e a troca de informações utilizam campos magnéticos ou eletromagnéticos.

O sistema de identificação por radiofreqüência tem mostrado inúmeras vantagens sobre os demais sistemas de identificação. Por isso, ele vem conquistando vários mercados, como o mercado de passagens para o transporte público de pequenas distâncias. Como exemplo, pode-se citar o Metrô de Brasília que já

utiliza no sistema de cobrança de passagens a tecnologia RFID de curto alcance. A tecnologia RFID será detalhada na próxima seção.

2.3 TENOLOGIA RFID

Um sistema RFID é composto por um transponder (tag) e por um leitor que podem trocar informações em um sentido (comunicação half duplex - da tag para o leitor) ou em dois sentidos (comunicação full duplex - da tag para o leitor e o leitor pode fazer escrita de dados na tag). Tanto na comunicação half duplex como na full duplex, a resposta do transponder se dá por meio de ondas de radiofreqüência em broadcast, quando o transponder está na zona de interrogação da leitora, figura 2.5.

Como a potência do sinal de resposta do transponder é bem inferior à potência emitida pelo próprio leitor, é necessário utilizar técnicas de modulação para diferenciação do sinal do transponder e do sinal do leitor. O uso de subportadora modulada é muito comum em transmissão de rádio. Em sistemas RFID é usada a modulação de carga com subportadora, que modula a subportadora inicialmente pelo sinal codificado em banda base e só depois realiza o chaveamento da carga, mas sempre usando harmônicos da freqüência de transmissão do leitor.

Figura 2.5: Infra-estrutura dos sistemas RFID.

2.3.1 Transponders

Transponder, RF tag ou simplesmente tag, é a etiqueta RFID em si. Sua estrutura básica é bem simples: um chip capaz de armazenar informações e uma impedância fazendo o papel de antena, protegidos por algum material, como plástico ou silicone, em determinado formato (chaveiro, etiqueta, cartões, entre outros), figura 2.6.

O transponder é responsável pela identificação de pessoa ou objeto que o tem em seu poder e que o identifica quando o mesmo passa pela zona de interrogação do leitor. Pode ser passivo ou ativo. Quando se trata de um transponder passivo, a etiqueta RFID não possui uma fonte de energia própria, sendo a energia necessária para a operação do transponder provida pelo campo elétrico ou magnético do leitor. No caso de um transponder ativo, a etiqueta RFID possui uma bateria própria para prover a alimentação necessária

Figura 2.6: Transponder (tag) RFID.

para o funcionamento das operações do microchip.

A capacidade de armazenamento de dados de uma tag RFID varia de poucos bytes a vários kilobytes. A exceção a essa regra é o chamado 1-bit transponder. Ele só é capaz de identificar para o leitor se há uma etiqueta RFID na zona de interrogação do leitor (transponder no campo do leitor) ou não (sem transponder no campo do leitor). Caso haja um transpoder na zona de interrogação do leitor, a mesma recebe o bit 1. Esse sistema é muito utilizado em lojas de departamento para a prevenção de furtos. Caso algum consumidor tente sair da loja com uma mercadoria que não foi paga e, por isso, não teve sua etiqueta RFID removida, ao passar pelos leitores que se encontram nas saídas da loja, o mesma emitirá um sinal sonoro para avisar que uma mercadoria está passando por ele sem ter tido sua etiqueta removida.

A possibilidade de escrita no transponder aumentou muito as possibilidades de utilização dos sistemas RFID. Em sistemas muito simples, as informações armazenadas no transponder (normalmente na forma de um número serial) são escritas nele no momento da fabricação e não pode ser alterado depois. Em transponders programáveis, o leitor tem a possibilidade de escrita na tag. Existe mais de uma forma para armazenamento de dados. Em sistemas RFID com acoplamento magnético, o uso de EEPROMs é dominante, porém, esse sistema tem a desvantagem do alto consumo de energia durante as operações de escrita e o número limitado de ciclos de escrita. Em sistemas microondas, é comum o uso de SRAMs (*Static Random Access Memory* - Memória Estática de Acesso Aleatório) para armazenamento de dados. Essa memória facilita os ciclos de escrita que são extremamente rápidos, porém, requer uma fonte de alimentação ininterrupta de uma bateria auxiliar para retenção das informações gravadas.

Em sistemas programáveis, o acesso à memória para leitura e escrita e qualquer autorização para pedido de leitura e escrita deve ser controlado pela lógica interna da portadora de dados. Em casos simples, essas funções podem ser realizadas por uma ou mais máquinas de estados. Todavia, máquinas de estados têm a desvantagem de serem inflexíveis a mudanças feitas nas funções programadas, sendo necessárias mudanças no hardware do chip. Isso significa relayout do circuito, acompanhado de gastos para confecção de novos hardwares.

Os microprocessadores eliminam as dificuldades de inflexibilidade impostas pelas máquinas de estado. Sistemas operacionais ficam responsáveis pelo manejo e armazenamento das informações relativas à aplicação. Logo, alterações na funcionalidade na tag tornam-se mais fáceis e mais baratas de serem implementadas, além do software possibilitar que adaptações sejam feitas para atender às mais diversas aplicações.

Para sistemas RFID (sistemas com troca de dados sem contato), os cartões que usam máquinas de

estados são conhecidos como cartões de memória e são bastante diferentes dos cartões microprocessados.

2.3.2 RFID Readers

O transceptor ou leitor é o componente de comunicação entre o sistema RFID e os sistemas externos de processamento de informações. A complexidade dos leitores depende do tipo de etiqueta (tag) e das funções a serem aplicadas. Os mais sofisticados apresentam funções de checagem (*check*) de paridade de erro e correção de dados.

Uma vez que os sinais do receptor sejam corretamente recebidos e decodificados, algoritmos podem ser aplicados para decidir se o sinal é uma repetição de transmissão de uma tag. Uma cabeça de leitura / escrita (ou apenas leitor) realiza a comunicação dentro do sistema de RFID e possui capacidade de processamento simples. A figura 2.7 ilustra um modelo de leitor RFID, destacando o sistema embarcado e a antena para aumentar o alcance.

Figura 2.7: Modelo de leitor para sistemas RFID.

2.3.3 Antena

A antena fica em um mesmo dispositivo junto com o transceptor e o decodificador, geralmente em configurações portáteis. A antena induz energia ao(s) transponder(s) para comunicação de dados dentro do campo de transmissão. Esses dados, depois de lidos, são passados ao controlador do sistema de RFID.

A antena emite um sinal de rádio que ativa a tag, realizando a leitura ou escrita. Essa emissão de ondas de rádio é difundida em diversas direções e em distâncias desde uma polegada até alguns metros, dependendo da potência e da freqüência usada. O tempo decorrido nessa operação é inferior a um décimo

de segundo, portanto o tempo de exposição necessário da tag é bem pequeno.

A função do leitor é ler e decodificar os dados que estão em uma tag que passa pela zona eletromagnética gerada pela sua antena. Os leitores são oferecidas em diversas formas e tamanhos conforme a exigência operacional da aplicação.

2.3.4 Controladores

O controlador de RFID é o dispositivo de interface que controla todo o sistema periférico de RFID (antena ou leitor e transponders) além da comunicação com o resto do sistema ou host. Existem vários controladores de RFID disponíveis para vários protocolos de comunicação. A figura 2.5 mostra o sistema de controle, normalmente realizado por um computador, em casos de sistemas mais simples, ou um servidor, para sistemas mais complexos.

Nos capítulos 3 e 4 será realizada uma abordagem mais aprofundada desses dispositivos.

2.4 PADRONIZAÇÃO DOS SISTEMAS RFID

Existem diversos fóruns de padronização do RFID, relativos tanto à tecnologia como à sua utilização. Alguns dos principais fóruns são: NFC Forum, EPC Global e ISO.

2.4.1 NFC Forum

A tecnologia NFC (*Near-Field Communication*) baseia-se em comunicação RF entre dispositivos eletrônicos móveis. A associação NFC Forum é voltada para a promoção da utilização de tecnologias de comunicação sem fio em curtas distâncias. A arquitetura proposta por essa associação inclui protocolos de como os dispositivos RFID estabelecerão comunicação, trocarão dados e interagirão. Inclui ainda a lista de todos os tipos de tags RFID que todos os dispositivos compatíveis com essa tecnologia devem ser capazes de ler [4].

Esta arquitetura está baseada em três modos principais de operação: *peer-to-peer*, *read-write* e *card-emulation*. As aplicações estão detalhadas abaixo:

1. *Peer-to-peer*: é utilizada para transmissão de dados entre dispositivos, como envio de informações de contatos ou um contrato eletrônico enviado de um dispositivo a outro. Pode ser usado também para conectar dois equipamentos para poderem intercomunicar-se.

2. *Read-write*: um dispositivo pode acessar os dados do outro.

3. *Card-emulation*: Um dispositivo emula um cartão de crédito que não exige contato visual, que pode ser usado para pagar produtos e serviços.

Cada um desses modos exige que os dispositivos read-write RFID utilizem formatos comuns de comunicação de dados. A primeira especificação, a de definição de gravação de dados, permite que os dispositivos se comuniquem utilizando linguagem comum. As próximas especificações definirão a maneira

como esses equipamentos conduzirão transações específicas. Esses procedimentos estão em processo de aprovação. O próximo passo será a definição de padrões para um protocolo do controle de conexão entre dispositivos peer-to-peer bem como card-emulation.

Os padrões estão sendo baseados em um espectro inicial de tags de alta freqüência (13,56 MHz). São eles ISO18092, ISO 14443-A e 14443-B, em conjunto à FeliCa Sony. Todos os dispositivos deverão ser capazes de ler e escrever nas tags que utilizam estes protocolos. O tipo de plano de licença, no entanto, ainda está em desenvolvimento.

O interesse da NFC Forum é de facilitar os padrões para os fornecedores ou fabricantes e promover assim a utilização de sistemas de comunicação wireless de baixa distância. Não será exigida a associação dessas companhias ao NFC Forum. As taxas para acesso aos protocolos ainda não foram definidas.

Desde 2002 a Philips investe em um padrão pioneiro aberto através da EMCA Internacional, resultando no Fórum de Comunicação de campo próximo [5]. Os principais membros deste fórum são: American Express, Anadigm, France Telecom, Innovision, Inside, LG, Logitech, Motorola, RFMD, SK Telecom, Skidata e Vodafone. Os padronizadores oficiais são: MasterCard International, Matsushita Electric Industrial, Microsoft, Nokia, NEC, Renesas Technology, Royal Philips Electronics, Samsung, Sony, Texas Instruments e Visa International.

O fórum explica como integrar sinalização ativa entre dispositivos móveis usando campo próximo (*Near Field Communication*). O objetivo é a busca de uma maneira mais fácil do usuário interagir com o meio informatizado, através de atividades simples, como um toque em objetos inteligentes, estabelecer comunicações ao se aproximar de um outro dispositivo, entre outros. Propõe também protocolos para troca de dados que interagem e serviços independentes aos dispositivos, assim como protocolos para dispositivos que ainda serão desenvolvidos e dispositivos que ainda serão capazes de utilizar o padrão NFC. O fórum também estabeleceu uma certificação para ter certeza da funcionalidade completa dos produtos de acordo com as suas especificações. Com isso, espera-se poder incentivar os fornecedores a desenvolver os seus produtos em um mesmo padrão fornecendo aos usuários possibilidade de integrar produtos de diferentes fornecedores.

Esse padrão RFID tenta promover o uso global da tecnologia RFID, fazendo com que os produtores e consumidores tenham conhecimento sobre esta nova tecnologia e busca oferecer um mecanismo padrão pelo qual dispositivos móveis sem fio podem se comunicar com outros dispositivos próximos (até 20 cm de distância). Mecanismos de busca de ondas de rádio, como Bluetooth e Wi-Fi, têm características de propagação imprevisíveis e podem se comunicar com dispositivos que não são locais. Os padrões NFC têm como objetivo modernizar ainda mais a tecnologia, passando endereços de controle de acesso de mídia sem fio e chaves de encriptação através do canal de comunicação, o que permite aos usuários reforçarem sua própria segurança física, apenas usando troca de chave de encriptação.

2.4.2 EPC Global

A EPC Global, coordenada pelo Auto-ID Center, é uma organização sem fins lucrativos que foi criada para administrar e incentivar o desenvolvimento da tecnologia RFID. Entre as inúmeras aplicações dessa tecnologia, a proposta da EPC Global é a padronização da tecnologia de comunicação de campo de longa distância, trabalhando na freqüência UHF para aplicações em gerenciamento da cadeia de suprimentos, já

que os investidores patrocinadores do laboratório projetista têm interesse em desenvolvimento voltado para seus segmentos de mercado.

Ela não padroniza o produto em si, mas a interface para comunicação entre os diversos componentes, estabelecida preferencialmente via Internet. Assim, existem protocolos distintos para comunicação entre a etiqueta e o leitor, entre o leitor e os computadores e entre computadores na Internet. A arquitetura do sistema de informações proposto pela EPC Global está descrita com maior detalhamento no capítulo 3.

NFC e o padrão EPC Global são incompatíveis. O EPC Global tem um fórum próprio, assim como NFC, onde ele discute sobre a padronização visando as mesmas praticidades que o NFC fornece, porém com um princípio de tecnologia diferente.

2.4.3 ISO

A ISO (*International Standards Organization*, é uma associação internacional de organismos de padronização. Ela não possui autoridade regulatória e limita-se à produção de normas, procedimentos e regulamentações em um amplo campo de assuntos e aplicações. Esses padrões internacionais fornecem os moldes para que cada membro possa desenvolver seus próprios padrões. As agências reguladoras podem adotar esses padrões ISO sem modificações, ou alterá-los para atender a condições locais. O resultado é que esses padrões tornam-se internacionalmente compatíveis, consistentes e claros.

A norma internacional ISO 11784, junto às normas ISO 11785 e 14223, descrevem a estrutura e a informação contidas no código de radiofreqüência utilizados na identificação de animais. Ela especifica o comprimento de 64 bits para a mensagem binária enviada pelo transponder para o transceiver, e o significado de cada bit dentro dessa seqüência. A mensagem é dividida em diferentes seções com significados específicos, incluindo a indicação de que o transponder é para uso animal, fabricante e/ou código do país, mais um código fixo de identificação do transponder. Existe também uma seção para identificação de erros (dígito verificador), que garante que a mensagem foi lida corretamente pelo transceiver e outras seções que ficam reservadas para uso futuro.

A norma ISO 11784 também especifica que é responsabilidade de cada país assegurar-se de que cada transponder carrega um código único dentro daquele país, e aconselha cada país a manter uma base de dados contendo informações sobre todos os números emitidos e os animais que foram associados a eles. No Brasil, a ABNT (Associação Brasileiras de Normas Técnicas) tem o papel de entidade reguladora das normas ISO, e já adotou a norma ISO 11784.

A norma ISO 11785 define os métodos de transmissão dos dados do transponder e as especificações dos leitores para ativação do transponder. A norma ISO 14223 define a interface de alta freqüência e a estrutura de dados para tipos específicos de transponders (avançados), sendo assim considerada uma evolução das normas ISO 11784 e 11785.

As normas 10536, 14443 e 15693 definem os padrões de comunicação de Smart Cards. A norma ISO 10536 define padrões de acoplamento a curta distância, hoje pouco usados devido ao alto custo de manufatura de cartões que utilizam essa tecnologia.

A norma ISO 14443 regula sobre cartões de identificação de curta distância. Ela possui determinados recursos que a tornam particularmente bem adequada a aplicações que envolvem informações de segurança,

como números de conta de cartão de crédito. Como resultado, a ISO 14443 é usado em mais de 80% das transações de cartão de crédito sem contato em todo o mundo. Adições recentes ao padrão permitem que a tecnologia ISO 14443 armazene dados biométricos como impressões digitais e fotos do rosto para uso em passaportes e outros documentos de segurança.

A norma ISO 15963 versa sobre comunicação entre smart cards próximos (cartões vizinhos), como aqueles usados em sistemas de controle de acesso. As portadoras de carga usadas nesses smart cards são módulos de memória de baixo custo baseadas em simples máquinas de estado.

O sistema ISO aponta outras organizações para acessar produtos ou serviços e certificar sua conformidade com alguma norma em particular. Nesse caso, é a organização certificadora que se torna legalmente responsável pela veracidade da certificação. Padrões ISO não possuem força de lei. Quando países, agências reguladoras ou usuários especificam que certos produtos ou serviços devam atender a uma o mais normas, essas organizações dão seu peso legal a essa decisão, e são elas mesmas responsáveis pelo cumprimento dessa lei ou regulamentação. Esse organismo tem em seu comitê técnico também a responsabilidade de desenvolver os padrões para os sistemas RFID [6].

2.5 APLICAÇÕES DOS SISTEMAS RFID

Os sistemas RFID podem ser empregados nos mais diferentes campos das aplicações comerciais, militares, entre outras. Será dado uma breve descrição das possíveis aplicações desse sistema para evidenciar sua importância [7].

2.5.1 Aplicações Médicas

Pesquisadores da área de saúde sugerem que, no futuro, um pequeno chip RFID implantado embaixo da pele poderá transmitir seu número e automaticamente acessar um completo registro de saúde do portador do chip. Funcionários do hospital, remédios e equipamentos também podem ser etiquetados, criando um potencial de administração automática, reduzindo erros e aumentando a segurança.

Chips do tamanho de um grão do arroz foram projetados para serem injetados no tecido do braço. Usando um leitor especial, os médicos e a equipe de funcionários do hospital podem buscar a informação, tais como a identidade do paciente, seu tipo sanguíneo e os detalhes de sua condição física, a fim de apressar o tratamento.

No caso de uma emergência, o chip pode salvar vidas, já que acaba com a necessidade de testes de grupo sangüíneo, alergias ou doenças crônicas, além de fornecer o histórico de medicamentos do paciente. Com isso, obtém-se maior agilidade na busca de informações sem a necessidade de localização dos prontuários médicos.

Uma outra aplicação médica é o implante de tags em humanos que contenham toda a informação de um paciente, podendo ser facilmente lida por um médico assim que o paciente chega ao hospital. Também na área médica, pode-se fazer uso de lentes especiais com um transponder implantado no olho de um paciente com glaucoma. O glaucoma é uma doença que vai tornando o campo de visão cada vez mais estreito, com o aumento da pressão interna do olho; mas as medições de pressão não podem ser feitas a não ser através

da cirurgia, portanto, o uso de uma micro tag com um medidor de pressão implantado no olho do paciente, como em uma cirurgia de catarata, pode comunicar-se com um leitor externo, fazendo assim medições exatas, salvando visões.

2.5.2 Implantes em Humanos

Figura 2.8: Implantes de transceptores RFID nas mãos de um usuário.

Implantes de chips RFID usados em animais agora estão também sendo usados em humanos. Um experimento feito com implantes de RFID foi conduzido pelo professor britânico Kevin Warwick, que implantou um chip em seu braço em 1998.

A empresa Applied Digital Solutions propôs seus chips (VeriPay) para debaixo da pele como uma solução para identificar fraude, segurança em acesso a determinados lugares, acesso a computadores, banco de dados de medicamento, iniciativas anti-seqüestro, entre outros, figura 2.8. Nesse caso, quando alguém for a um caixa eletrônico, bastará fornecer sua senha bancária e um scanner varrerá seu corpo para captar os sinais de radiofreqüência que transmitem os dados de seu cartão de crédito.

O Baja Beach Club, uma casa noturna em Barcelona, na Espanha, e em Rotterdam, na Holanda, usa chips implantado em alguns de seus freqüentadores para identificar os VIPs.

Em 2004 um escritório de uma firma mexicana implantou 18 chips em alguns de seus funcionários para controlar o acesso a sala de banco de dados.

Especialistas em segurança alertam contra o uso de RFID para autenticação de pessoas devido ao risco de roubo de identidade. Seria possível, por exemplo, alguém roubar a identidade de uma pessoa em tempo real. Devido ao alto custo, seria praticamente impossível se proteger contra esses ataques, pois seriam necessários protocolos muito complexos para saber a distância do chip.

2.5.3 Aplicações Industriais

A indústria de transporte é uma, entre muitas, que pode se beneficiar com uma rede de leitores RFID do tipo estáticos. Por exemplo, veículos de transportes de carga podem conter leitores internos para controle da mercadoria, figura 2.9.

Empresas locadoras de veículos podem fixar etiquetas RFID nos pára-brisas de carros, com a identificação do veículo. Assim, podem obter relatórios automaticamente usando leitores nos estacionamentos, além de ajudar na localização dos carros.

As empresas aéreas também podem explorar os leitores estáticos. Colocando RFID nas bagagens, pode-se diminuir consideravelmente o número de bagagens perdidas, pois os leitores identificariam o destino das bagagens e as direcionariam de forma mais eficiente.

Mais uma aplicação é a identificação de ferramentas, que no caso de grandes indústrias facilita o processo tanto de manutenção, quanto de substituição e administração das mesmas. Um outro campo que sistemas RFID podem tanto melhorar a rapidez e qualidade do serviço, como também ter um papel de segurança nas indústrias, é na identificação de recipientes, embalagens e garrafas, principalmente em produtos químicos e gases, onde um erro na hora de embalar pode causar sérios danos.

Hoje em dia, a maioria dos sistemas que gerencia recipientes é baseada em código de barras, porém, no meio industrial, o uso desse tipo de sistema não é confiável o suficiente, e os transponders de um sistema RFID podem guardar mais informações úteis posteriormente, como o dono do recipiente, conteúdo, volume, preenchimento ou pressão máximos e dados de análise, além dos dados poderem ser mudados e um mecanismo de segurança poder ser implementado, evitando escrita ou leitura não autorizadas. As tags usadas são de acoplamento indutivo, trabalham em uma faixa de freqüência inferior a 135 kHz e devem aceitar condições hostis, como poeira, impactos, radiação, ácidos e temperaturas muito altas ou muito baixas (de -40^{o}C a +120^{o}C).

Nessa área, a eliminação de lixo pode fazer uso de sistemas RFID, devido ao custo de despejo e o crescente rigor nas legislações ambientais. Com um melhor gerenciamento do lixo, como cálculo automático de quantidade e manutenção dos aterros sanitários, ajuda a distribuir responsabilidades e custos de maneira mais crível. Além de ajudar em sistemas de gerenciamento ambiental, tanto no Brasil como em outras partes do mundo, a legislação prevê penas a quem de alguma forma danifica o meio, já que a Constituição Federal prevê que o meio ambiente é bem de uso comum do povo. O Brasil dispõe, em sua Constituição, regras quanto a pesquisa, a experimentação, a produção, a embalagem e rotulagem, o transporte, o armazenamento, a comercialização, a propaganda comercial, a utilização, a importação, a exportação, o destino final dos resíduos e embalagens, o registro, a classificação, o controle, a inspeção e a fiscalização de agrotóxicos, seus componentes e afins, entre outras providências. Em algumas cidades do mundo, já existem sistemas RFID para controle de lixo, onde as tags são colocadas nas latas de lixo e os caminhões de coleta tendo leitores.

2.5.4 Aplicações em Celulares

Os leitores de RFID do tipo móveis podem ser instalados em aparelhos que fazem parte do dia-a-dia das pessoas, como os celulares. Colocando um desses celulares em frente a um produto com etiqueta RFID

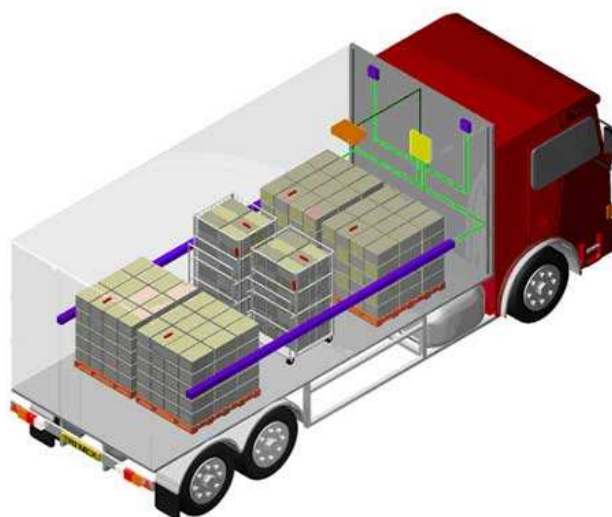



Figura 2.9: Caminhão equipado com leitores RFID.

obtém-se seu preço, por exemplo, assim como suas especificações. O celular também pode ser usado para compras, através da leitura do RFID, de um determinado produto. A companhia de cartão de crédito efetua o pagamento por meio da autorização do celular.

Um exemplo de aplicação para RFID em celulares é o check-in em hotéis. Assim que o hóspede faz o check-in, o hotel envia o número do quarto e a "chave" para o celular do hóspede. Este se encaminha para o quarto e usa seu celular para destravar a porta.

Em 2004, a Nokia anunciou o celular 3200 GSM, que incorpora um leitor NFC. Embora a empresa não tenha publicado uma extensiva lista de aplicações potenciais, o telefone pode fazer pagamentos eletrônicos (similar a um smartcard) e fazer chamadas baseado no encontro de tags de RFID. Por exemplo, colocando-se o telefone próximo a uma tag RFID existente numa placa de ponto de táxi e o telefone chamaria a companhia de taxi e pediria um táxi naquele local. Este modelo oferece uma ligação entre um representante virtual com uma memória de um computador, e a posição do táxi começa a ser traçada com o disparo do computador, e no mundo físico, com um sinal e pessoas com celulares. Além disso, é uma chave habilitando a implementação da tecnologia.

2.5.5 Aplicações em Bibliotecas

Em bibliotecas e centros de informação, a tecnologia RFID é utilizada para identificação do acervo, possibilitando leitura e rastreamento dos exemplares físicos das obras. Funciona fixando-se uma etiqueta RFID (tag) plana (de 1 a 2 mm), adesiva, de dimensões reduzidas (50 x 50 mm em média), contendo no centro um micro-chip e ao redor deste uma antena metálica em espiral. Um conjunto com sensores especiais e dispositivos fixos (portais), de mesa ou portáteis (manuais), possibilitam a codificação e leitura dos dados dos livros na tag, principalmente seu código identificador - antes registrado em códigos de barras.

A etiqueta é inserida normalmente na contracapa dos livros, perto da lombada, dentro de revistas e sobre materiais multimídia (CD-ROM, DVD) para ser lida à distância.

É possível converter facilmente os códigos identificadores existentes atualmente no código de barras

para etiquetas RFID usando-se equipamentos próprios para esta conversão. Algumas aplicações em bibliotecas são: auto-atendimento; controle de acesso de funcionários e usuários; devolução e empréstimo; estatística de consulta local; leitura de estante para inventário do acervo; localização de exemplares mal-ordenados no acervo; localização de exemplares em outras bibliotecas da rede e re-catalogação, figura 2.10.

Apesar de ser possível o uso de etiquetas de RFID para segurança anti-furto de acervo (algumas etiquetas permitem gravar a informação se o acervo está ou não emprestado em um bit de segurança), este uso não é recomendado, devido ao fato de qualquer barreira metálica poder "blindar"ou bloquear os sinais de rádio impossibilitando a leitura da etiqueta [8].

Figura 2.10: Exemplo de aplicação RFID em uma biblioteca.

2.5.6 Aplicações na Área de Segurança

Além do controle de acesso, um sistema RFID pode prover, na área de segurança, outros serviços. Um deles é o sistema de imobilização. No início dos anos 90, o roubo de carros cresceu, tornando promissor o mercado de segurança para carros, alarmes e sistemas de imobilização. Os controles de alarme com alcance de 5 a 20 metros estão no mercado há anos. São pequenos transmissores de radiofreqüência que operam em 433,92 MHz. Nesse tipo de sistema de segurança para carros, somente esse controle pode acionar o destravamento do carro, permitindo que ele seja aberto. Sem que um ruído, o alarme, seja emitido as portas destravam. Impedir que o carro seja ligado é trabalho do sistema de imobilização. Se o controle que o destrava for quebrado, o carro ainda assim pode ser aberto através das chaves, por um processo mecânico, mas não há como o sistema reconhecer se a chave inserida é genuína. Nesse caso, uma ferramenta específica ou uma chave-mestra pode abrir o veículo. A tecnologia dos transponders de RFID pode agir justamente nesse ponto, verificando a autenticidade da chave. Então, o sistema antigo cuida do alarme e destravamento e a tag RFID da imobilização. Assim, se uma chave, que não for a original do carro, tentar ligá-lo, o carro é imobilizado, mesmo que o alarme tenha sido desligado e as portas abertas. Mobilização Eletrônica é o nome dado a este sistema, onde o sistema de ignição é combinado com um transponder, incorporado diretamente na chave.

2.5.7 Aplicações em Identificação Animal

A identificação dos animais por sistemas RFID ajuda no gerenciamento dos mesmos entre as companhias, no controle de epidemias e garantia de qualidade e procedência. Essa identificação pode ser feita de quatro maneiras diferentes: colares, brincos, injetáveis ou ingeríveis (bolus). Os colares são fáceis de serem aplicados e transferidos de um animal para o outro; é usado geralmente apenas dentro de uma companhia. No caso dos brincos, são as tags de menor custo, e podem ser lidas a uma distância de até um metro. No caso das tags injetáveis, que são usadas a cerca de 10 anos, ela é colocada sob a pele do animal com uma ferramenta especial, um aplicador parecido com uma injeção. A tag ingerível, ou bolus, é um grande comprimido revestido geralmente por um material cerâmico resistente a ácido e de forma cilíndrica, e pode ficar no estomago do animal por toda sua vida.

2.5.8 Aplicações em Manutenção

As principais preocupações em um processo de manutenção de sistemas complexos podem ser sumarizadas em informações precisas e atuais sobre os objetos; transferência em tempo real das informações dos incidentes críticos; e acesso rápido às bases de conhecimento necessárias para a solução do problema.

Um dos aspectos interessantes do RFID é a possibilidade de manter um histórico de manutenção no próprio objeto. Outro aspecto é a segurança, pois o RFID encontra-se embarcado no objeto. Dessa forma, ações fraudulentas são coibidas de maneira mais eficaz. Como cada objeto possui um único RFID, não clonável, os prestadores de serviços não podem ludibriar os relatórios de manutenção, objetivando maiores ganhos financeiros.

O RFID ainda propicia uma melhora na documentação do processo de manutenção, permitindo relatórios mais eficientes, além de uma redução dos custos administrativos em decorrência da diminuição da burocracia.

Devido à grande preocupação com uma manutenção ágil e eficiente nas instalações aeroportuárias, o RFID torna-se uma alternativa interessante, já que provê facilidades para identificação, localização e monitoramento de objetos físicos. O aeroporto de Frankfurt (Franport), o segundo maior da Europa, com movimento superior a 50 milhões de passageiros por ano, iniciou um projeto piloto em 2003 com o objetivo de testar os benefícios do RFID nas suas dependências.

A manutenção no Fraport é sobrecarregada, pois mais de 450 companhias são envolvidas no processo. Com o advento do RFID, o aeroporto começou a se modernizar: os técnicos de manutenção agora usam dispositivos móveis para acessar os planos de manutenção e registrar as ordens de serviço. Todos os 22 mil extintores de incêndio foram equipados com RFID, identificando o histórico de manutenção, incluindo a última data de inspeção.

Diariamente os técnicos percorrem o aeroporto efetuando as tarefas de manutenção necessárias. Para tal, os técnicos se autenticam nos dispositivos móveis (usando também RFID), recebendo suas atividades do dia. Após o término da checagem de cada equipamento escalonado para sua inspeção, o técnico registra seu RFID uma segunda vez, criando, assim, um registro de manutenção.

Observando o caso de sucesso de Frankfurt, fica evidente que o RFID, de fato, pode otimizar os processos de manutenção. Conseguiu-se um ganho extraordinário de eficiência administrativa ao introduzir tal

tecnologia nos extintores, uma tarefa que outrora consumira 88 mil páginas de papel que eram arquivados por ano. Isso passou a ser feito de forma automática e com baixo custo.

2.6 SEGURANÇA

As modernas etiquetas RFID representam a evolução da tecnologia e do baixo custo da computação embarcada. Além disso, têm o tamanho de um grão de arroz e possuem lógica embutida, elementos acoplados e memória. Entretanto, apesar de apresentar grandes progressos na vida cotidiana das pessoas, tal tecnologia pode trazer grandes problemas aos seus usuários.

As etiquetas RFID possuem um grande problema: não contém nenhuma rotina ou dispositivo para proteger seus dados. Mesmo as etiquetas passivas, que têm raio de ação de poucos metros, podem sofrer interceptação e extravio de suas informações. Pensando em etiquetas ativas, o problema torna-se bem mais crítico.

A fabricante de tags RFID Alien Technologies diz que as tags podem ser lidas de distâncias de até 4,5 metros. Porém, quando existem obstáculos entre o leitor e o emissor, esta distância diminui. Assim, para que criminosos possam fazer uso do RFID para praticar suas ações, eles teriam que possuir um receptor muito mais sensível do que o normal.

Se a tecnologia RFID realmente tomar as proporções esperadas, toda pessoa terá etiquetas em seus objetos e até em seu próprio corpo. Assim, dados pessoais poderão ser obtidos por qualquer pessoa que tiver em mãos um leitor RFID. Para que isso não ocorra, soluções já vêm sendo estudadas e testadas (talvez o segredo não esteja em armazenar informações no tag de identificação e sim no leitor ou em um computador).

O RFID tem como característica básica armazenar dados do material em que está aplicado. Além disso, tal material pode ser facilmente rastreado. Portanto, a implantação desta tecnologia sem um tratamento cuidadoso em segurança pode acarretar em graves problemas aos seus usuários [9]. Resumidamente, os problemas que podem surgir com esta tecnologia são:

- Violação da integridade física: uma etiqueta possui dados específicos do material em que está localizada. Se esta for colocada em outro material, pode causar danos ao seu usuário. Um exemplo: se um ladrão trocar a etiqueta de um produto caro (ex: televisão) com a de um produto barato (ex: pilha), poderá lesar o estabelecimento.
- Cópia de etiquetas: sendo detentora do conhecimento de criação de etiquetas, uma pessoa pode copiar dados de uma etiqueta alheia, usando um leitor, e criar uma nova com os mesmos dados.
- Monitoramento da etiqueta: obtenção de dados das etiquetas para uso indevido sem envolver fisicamente a etiqueta. Exemplo: um seqüestrador pode rastrear os dados bancários de uma pessoa e, sabendo que esta possui grande quantia de dinheiro, obrigar que ela saque o dinheiro em caixa eletrônico.

Esses são alguns dos problemas que possivelmente trarão mais complicações às pessoas caso a tecnologia RFID seja implantada em larga escala e sem ter o devido cuidado em segurança.

2.7 ATAQUES E VULNERABILIDADE

Os sistemas de RFID são divididos em quatro zonas de segurança, as quais devem ser separadamente analisadas e protegidas. Cada zona assume uma determinada quantidade de conexões confiáveis com outros elementos (outras zonas), e impede que elementos de fora tenham tais privilégios.

A Zona 1 compreende as próprias tags RFID. Existem duas áreas onde podem haver possíveis vulnerabilidades. Uma delas é quando os dados da tag são guardados de forma não encriptada. Isso pode acontecer porque encriptar dados em uma tag aumenta os gastos com espaço e com os circuitos. A outra vulnerabilidade possível é quanto ao acesso físico, onde uma pessoa pode retirar uma tag de um artigo ou trocá-la. Para corrigir essas vulnerabilidades, pode-se ter um controle físico de acesso apropriado, implementar segurança nas mercadorias etiquetadas com RFID, separar o código EPC de informações restantes que sejam sensíveis à empresa e aos consumidores, e por fim, somente usar tags que permitem reescrita onde há controle de acesso físico e encriptação. Por exemplo, se alguém com acesso indevido entrar em um armazém que antecede uma esteira, retira a tag de um produto e o coloca em outro, pode roubar este artigo sem que a sua falta seja dada tão cedo. Outro exemplo é o de alterações nos dados da própria tag, onde uma pessoa pode alterar o seu conteúdo, como o preço, ou simplesmente trocar a tag com um produto de preço menor.

A Zona 2 compreende os leitores, geralmente conectados à uma rede local através de redes comuns ou wireless. As vulnerabilidades podem ser: o tráfego de informação entre o leitor e as tags não é encriptado, ou os leitores não autenticam as tags, o que pode levar a ataques como spoofing (tag falsa) ou por Denial Of Service (DoS, Negação de Serviço). Qualquer pessoa conectada à mesma rede que os leitores, ou nas proximidades (no caso de redes wireless), com alguma ferramenta de sniffer (ferramenta que busca por dispositivos conectados à rede) pode atacar. Encriptar a comunicação entre os leitores e as tags, mecanismo de autenticação para as tags, necessidade de autenticação e autorização para acessar os serviços dos leitores, segurança nos Access Points no caso de redes wireless e protocolos anti-colisão ajuda a prevenir tais problemas. Um ataque pode ser feito em uma rede wireless no caso de um intruso interferir na comunicação com um ruído ou usar uma tag que bloqueie o sinal das demais. No caso da rede, um dos nós da mesma rede pode tentar obter acesso aos serviços do leitor, ou simplesmente monitorar as informações que estão passando por ele.

Na Zona 3, estão os serviços como ONS (*Object Naming Service* - Serviço de Nomeação de Objetos), Gerenciador de Eventos, EPCIS e o servidor de integração. ONS é um serviço da EPC Global Inc que funciona na tradução de um código EPC para a informação de um produto. É como um DNS, mas para objetos. EPCIS (*EPC Information Service*) é um repositório de eventos de RFID EPC. O Security Working Group da EPC é um grupo que trabalha na segurança dos sistemas RFID EPC. São ajudados pela VeriSign e ConnecTerra. Dentre as vulnerabilidades, estão os próprios serviços, tanto internos da empresa, utilizando LANs ou WANs, quanto os sistemas aos quais estão conectados, como de indústrias e parceiros. Permite trabalho de espiões corporativos, agentes de espionagem e intrusos. Medidas de controle de acesso à rede, como firewalls, softwares de detecção de intrusos, sniffers, acesso físico, e também seguir as recomendações da Security Working Group da EPC ajudam a evitar ataques.

A Zona 4 compreende os sistemas corporativos, como gerenciamento de diretório, de identidade, acesso de controle e sistemas mensageiros. Um sistema RFID aumenta o fluxo de volume de dados e

transações em uma empresa, o que pode ocasionar uma sobrecarga na sua infra-estrutura, tornando este um ponto vulnerável por não estarem preparadas para esse volume de informação. Controle de acesso à rede, implementar firewalls, detecção de intrusos, sniffers e acesso físico evita acessos indevidos. Os problemas podem ocorrer devido ao fluxo de informação e a quantidade e rapidez com a qual são adicionados no sistema são muito mais rápidas do que nos códigos de barras.

Em meio a tantas possibilidades de violação da segurança, existem estudos para que a tecnologia RFID seja implantada sem causar danos aos seus usuários. Isso faz com que seu uso em larga escala seja viável e que a vida das pessoas seja facilitada sem nenhum transtorno. Algumas possíveis soluções são:

- **Criptografia**: assim como é utilizado nas mensagens eletrônicas (e-mails), o advento da tecnologia faz com que somente emissor e receptor possam ter acesso à informação contida na etiqueta. Qualquer pessoa que tentar obter esses dados ilicitamente terá que decifrar um código já comprovadamente altamente confiável (ex: RSA).
- **Códigos**: neste caso, o conteúdo da etiqueta só poderia ser usado mediante o uso de um código. Por exemplo: em um supermercado, o usuário deveria usar um código para liberar a compra usando RFID.
- **Dispositivos metálicos**: envolvida com estojo feito de um material reflexivo (estudos indicam o alumínio), a etiqueta ficaria livre de interceptações quando não estivesse em uso.

Tais soluções não garantem segurança total no uso das etiquetas RFID, mas fazem com que esta tecnologia se torne mais confiável.

2.8 QUESTÕES ÉTICAS E PRIVACIDADE

Como se sabe, as tags RFID podem ser usadas para uma série de funções como controle de estoque e identificação de propriedade prevenindo roubo ou perda. Ou seja, são muito úteis. Uma loja poderia, por exemplo, colocar tags RFID em todos os seus produtos e os clientes poderiam ter um cartão de crédito que automaticamente debitaria o valor das compras na hora que o cliente saísse da loja, sem precisar passar pelo caixa. E aí que começam os problemas.

O que acontece, por exemplo, se uma loja de roupas decide colocar esses tags invisíveis em todas as roupas. Você compra e leva para casa. Um belo dia, você retorna à loja usando aquela mesma roupa e é reconhecido pelo nome. Ou entra em uma loja de departamentos e recebe sugestões em grandes painéis baseado em compras passadas. Mesmo com regulamentação governamental, a situação pode se tornar rapidamente uma ameaça à privacidade. Principalmente quando criminosos começarem a se aproveitar da tecnologia.

A ameaça à privacidade vem quando o RFID permanece ativo quando o consumidor deixa o estabelecimento. Este é o cenário que deve alarmar as pessoas - e, no momento, a indústria de RFID parece dar sinais mistos sobre a ativação das tags - se devem ser desativadas ou deixadas ativadas por padrão.

Uma das possibilidades seria a de deixar o cliente escolher se quer manter suas tags ativadas ou não, e informar ao estabelecimento caso este opte por desativá-las.

Para respeitar a privacidade dos consumidores, os estabelecimentos devem seguir estas 4 premissas:

- Os consumidores devem ser notificados quanto à presença de RFID nos produtos, e em quais deles isto acontece;
- Tags RFID devem ser desativadas na saída do caixa do estabelecimento;
- Tags RFID devem ser colocadas na embalagem do produto, e não nele próprio;
- Tags RFID devem ser bem visíveis e facilmente removíveis.

3 CONTROLADORES RFID

3.1 INTRODUÇÃO

Os sistemas RFID podem, quando solicitados, obter informações dos objetos rastreados quase em tempo real. Essas informações, no entanto, devem ser gerenciadas e manipuladas, de forma a garantirem um sistema viável.

Toda a estrutura de hardware do sistema, bem como todas as aplicações, exigem certo processamento dos dados, de acordo com a demanda. As informações, por exemplo, depois de gravadas na tag, devem ser enviadas aos leitores, respeitando as solicitações. O funcionamento dos leitores e das tags depende de seus fabricantes, mas o controle, gerenciamento e atualização são responsabilidades do usuário, ou, na maioria das vezes, das empresas que empregam o sistema RFID.

Para facilitar a atividade dos detentores de sistemas RFID, alguns softwares de gerenciamento de dados foram desenvolvidos. Esses sistemas geralmente são flexíveis em relação ao aplicativo a que se destinam. Em contrapartida, a complexidade está diretamente ligada ao dispositivo a ser gerenciado e, em segundo plano, ao apelo comercial a ser dado ao software.

A IBM desenvolveu uma plataforma completa para a implementação de um sistema RFID fim a fim – *IBM RFID Solution* (Solução RFID IBM) –, composta por um conjunto de aplicativos, softwares e dispositivos de hardware baseados em sistemas IBM. A interação entre estes dispositivos e as funções por eles desempenhadas torna essa solução quase universal, ou seja, permite que ela seja utilizada em quase todas as aplicações RFID possíveis. Para que o máximo desempenho seja atingido, no entanto, a IBM recomenda que toda a infra-estrutura seja do mesmo fabricante. Um grande foco comercial também é dado a essa plataforma, pois permite que funções empresariais muito distantes da esfera da tecnologia RFID sejam executadas paralelamente. Todas as características e funções apresentadas fazem com que essa plataforma, apesar de completa, seja consideravelmente complexa e, conseqüentemente, dispendiosa financeiramente para o investidor interessado em controlar seu sistema.

O Auto-ID center (Auto-ID Labs) também em busca de controle de dados desenvolveu um software denominado *Savant Concentrator* (Concentrador Savant). A idéia principal desse sistema é realizar filtragens sucessivas, com processamento dos dados obtidos nos estágios intermediários, o que permite confiabilidade. Esse dispositivo foi criado em ambiente de desenvolvimento da tecnologia RFID. É uma solução mais simples que a solução IBM e ainda encontra-se em desenvolvimento. A ênfase comercial do Savant é ínfima quando comparado ao controlador IBM, já que o foco principal deste centro tecnológico não é vendas. O Auto-ID center busca atender a necessidade dos investidores, a partir da evolução da tecnologia RFID. O Savant Concentrator é somente uma ferramenta necessária para o enriquecimento da tecnologia como um todo [10].

Este capítulo trata desses softwares controladores de fluxo. Suas principais características são destacadas e o processamento das informações provenientes das tags é discutido. As informações deste capítulo são baseadas nos textos *IBM WebSphere Handbook* [11] e *Auto-ID Savant Specification* [12].

3.2 SOLUÇÃO IBM

A estrutura - *framework* - criada pela IBM para modelar a solução para controlador RFID fim-a-fim por ela implementada está ilustrada na figura 3.1. Nesse framework, o modelo (*RFID Solution Domain*) agrupa as soluções lógicas próximas, correlatas, em domínios por componentes. Ele modela o sistema completo. Esses domínios por componentes são projetados para atender às demandas das empresas e, ao mesmo tempo, dar suporte aos padrões em desenvolvimento como o EPC Global e o padrão ISO, promovendo o isolamento de avanços tecnológicos de um domínio sem afetar os demais domínios.

A arquitetura da solução IBM inclui os domínios do Objeto Rastreado (*Tagged Object*), do Leitor e da Antena (*Reader and Antenna*), da Interface de Comunicação (*Edge*), das Premissas (*Premises*), da Integração dos Processos Comerciais (*Business Process Integration*), das Aplicações Empresariais e Comerciais (*Enterprise and Business Application*), do Gerenciamento de Sistemas (*System Management*) e do Diretório do Objeto (*Object Directory*). O Gerenciamento da Segurança e Privacidade (*Security and Privacy Management*) faz parte desse modelo e está distribuído entre todos os domínios citados. Para cada domínio, a segurança e a privacidade são aplicadas de forma específica.

Figura 3.1: Modelo da solução para controlador RFID da IBM

1. Domínio do Objeto Rastreado (*Tagged Object*)

   Esse domínio contém os produtos rastreados da cadeia de produção ou qualquer outro objeto ou recurso que se deseje rastrear ou monitorar. Devido ao fato de o objeto e a tag estarem fisicamente unidos, eles são considerados pertencentes ao mesmo domínio.

   Diferentemente dos demais domínios, a maioria dos componentes pertencentes a esse domínio é móvel, o que implica que eles podem se locomover por diferentes infra-estruturas RFID. Essa característica dos componentes desse domínio impõe que eles tenham requisitos de interoperabilidade entre as diversas infra-estruturas RFID pelas quais eles possam passar. Para isso, é desejável que esses objetos sejam endereçados utilizando padrões abertos.

2. Domínio do Leitor e da Antena (*Reader and Antenna*)

   O domínio do Leitor e da Antena é a interface entre o mundo físico dos objetos, das freqüências

de rádio, das tags e das antenas e o mundo dos softwares. Espera-se que, no futuro, esse domínio seja mais complexo e comporte funcionalidades hoje executadas pelo domínio da Interface de Comunicação (Edge Domain). Para isso, é necessário que os leitores sejam mais complexos, capazes de serem mais seletivos aos sinais recebidos.

3. Domínio da Interface de Comunicação (*Edge*)

   O Domínio da Interface de Comunicação é responsável por filtrar e agregar a grande quantidade de dados que são adquiridos pelo sistema por meio do leitor. Esse domínio deve ter um dispositivo provido de inteligência para suportar a análise de dados e ser capaz de aplicar decisão, figura 3.2. A arquitetura dele precisa ser compatível com vários modelos de leitores de diferentes fabricantes e deve utilizar leitores e também ter interface com a tag que sejam particularmente eficientes com o restante da infra-estrutura.

   As funções do Domínio da Interface de Comunicação são tipicamente implementadas em aplicações de baixo custo e usam tecnologias de software embarcado para manter estável a pilha de processos que estão fora da fronteira da infra-estrutura RFID. Para possibilitar o gerenciamento de uma produção que é acompanhada por sistema RFID, a distribuição é um aspecto fundamental. Atualizações em softwares no Domínio da Interface de Comunicação devem ser distribuídas automaticamente.

Figura 3.2: Exemplo de dispositivo para interface de comunicação.

4. Premissas (*Premises*)

   O Domínio das Premissas é um domínio intermediário entre o de Integração dos Processos Comerciais e o da Interface de Comunicação. Promove a filtragem dos dados, monitora e escala eventos RFID com o objetivo de detectar operações comerciais críticas, possibilitando a tomada de decisões. Ele também monitora e registra toda informação relevante e importante sobre os produtos e suas localizações, além de gerenciar os componentes que estão em domínios anteriores (usando como base o modelo das soluções nos Domínios RFID da IBM) ao Domínio das Premissas, como os Leitores e os Controladores RFID.

   O Domínio das Premissas trata os eventos em um nível mais elevado que o Domínio da Interface de Comunicação. Isto é, trata os eventos que são importantes para a operação ou processo comercial. Este domínio é capaz de armazenar dados e pode interagir com os sistemas back-end (banco de dados) de uma empresa por meio da Integração dos Processos Comerciais.

5. Integração dos Processos Comerciais (*Business Process Integration*)

   O Domínio da Integração dos Processos Comerciais faz a união entre a infra-estrutura do sistema RFID e as aplicações empresariais. Enquanto os outros domínios mencionados anteriormente provêem o mínimo de funcionalidade ao sistema sem modificações na suas estruturas e independentemente da aplicação à que o sistema é destinado, a Integração dos Processos Comerciais, via de regra,

requer customização para suportar e oferecer um ambiente adequado às atividades desenvolvidas pela empresa. Por isso, esse domínio é descrito como uma caixa de ferramentas (toolbox) para a integração comercial.

Uma característica importante do Domínio da Integração dos Processos Comerciais é sua habilidade de agir como um disseminador das informações nas transações automáticas entre os sócios participantes de um negócio. Enquanto o resto da infra-estrutura RFID verifica movimentação em grande escala de produtos (um carregamento de navio, por exemplo), este domínio cria e envia mensagens (uma observação avançada de um navio, por exemplo) para o sócio interessado.

O Domínio da Integração dos Processos Comerciais não apenas conecta aplicações já existentes, mas pode também possibilitar a criação de novas formas de gerenciar e controlar negociações por meio de análises comerciais relacionadas ao RFID para monitorar os indicadores chaves de desempenho.

6. Aplicações Empresariais e Comerciais (*Enterprise and Business Application*)

   O Domínio das Aplicações Empresariais e Comerciais inclui as aplicações já existentes que precisam das informações sobre a movimentação dos produtos providas pela infra-estrutura RFID. Essas aplicações correspondem a uma variedade de requisitos comerciais que uma organização necessita.

   Esse domínio inclui sistemas que ajudam a ordenar, gerenciar ou suprir bens e que podem ser atualizados rapidamente para monitorar automaticamente a movimentação de produtos. Exemplos desses sistemas de ordenamento, gerenciamento e suprimento de bens são: Automação de Processos, Gerenciamento de Inventário, Planejamento dos Recursos da Empresa (*Enterprise Resource Planning* - ERP), Sistemas de Execução da Manufatura, Sistemas de Execução da Cadeia de Suprimentos, Sistemas de Gerenciamento do Armazém, Armazenamento dos Dados do Armazém, Sistemas da Loja, Processo de Trabalho na Produção, entre outros.

7. Gerenciamento de Sistemas (*System Management*)

   O Domínio do Gerenciamento de Sistemas permite aos clientes utilizar os sistemas RFID e mantê-los funcionando. Ele permite desenvolver e gerenciar aplicações remotamente em um ambiente distribuído, incluindo a habilidade de monitorar, configurar ou atualizar softwares e firmwares remotamente em recursos desenvolvidos tais como antenas, leitores e servidores. Este domínio pode incluir um painel central através do qual é possível monitorar recursos e receber alertas quando leitores, antenas e servidores param de funcionar. Os painéis ajudam a aumentar a confiabilidade e reduzir custos operacionais.

8. Diretório de Objeto (*Object Directory*)

   O Domínio do Diretório do Objeto fornece informações sobre a estrutura física do objeto que está portando sua identificação única como chave. Ele permite a rápida recuperação de informações e também fornece uma estrutura - framework - para permitir às empresas compartilhar de forma acertada informações sobre produtos com os parceiros comerciais. A Rede EPC é um exemplo de Domínio do Diretório do Objeto. Ele é composto por:

   - Serviço de Nomeação de Objeto - *Object Naming Service (ONS)*
   - Serviço de Descoberta do Código Eletrônico do Produto - *Eletronic Product Code Discovery Service (EPCDS)*

- Serviço de Informação do Código Eletrônico do Produto - *Eletronic Product Code Information Service (EPCIS)*

Este domínio tipicamente entrega três tipos de informações sobre o produto: núcleo do produto, tempo de produção e a história do ciclo de vida. Informação do núcleo do produto é normalmente obtida dos gerenciadores das informações do produto, catálogos de produtos ou união de dados.

9. Gerenciamento da Segurança e Privacidade (*Security and Privacy Management)*

   Como o RFID se transforma em parte integrante de um sistema de gerenciamento em larga escala dos dados dentro da empresa, sistemas de TI devem ser resistentes a falhas na segurança e na privacidade. Segurança efetiva e gerenciamento de privacidade permitem aos clientes aumentar a infra-estrutura de segurança já existente no leitor para a rede de Código Eletrônico do Produto - *Electronic Product Code (EPC)*. Essa infra-estrutura deve proteger os dados armazenados assim como os dados que estão em trânsito.

3.2.1 Implementação do Software Controlador da IBM

Para a implementação da solução da IBM, vários softwares são utilizados, aplicados aos domínios específicos. O middleware WebSphere Solution é utilizado especificamente para fornecer a infra-estrutura primordial para a implantação do sistema RFID.

O *WebSphere RFID Solution* consiste em três componentes: *WebSphere Premises Server*; *WebSphere Device Infrastructure*; *WebSphere Business Integration*. A figura 3.3 ilustra a distribuição desses componentes no quadro de domínios. Esse aplicativo IBM se destina à conexão do mundo físico RFID ao mundo de TI preexistente na empresa em que se aplica a solução RFID.

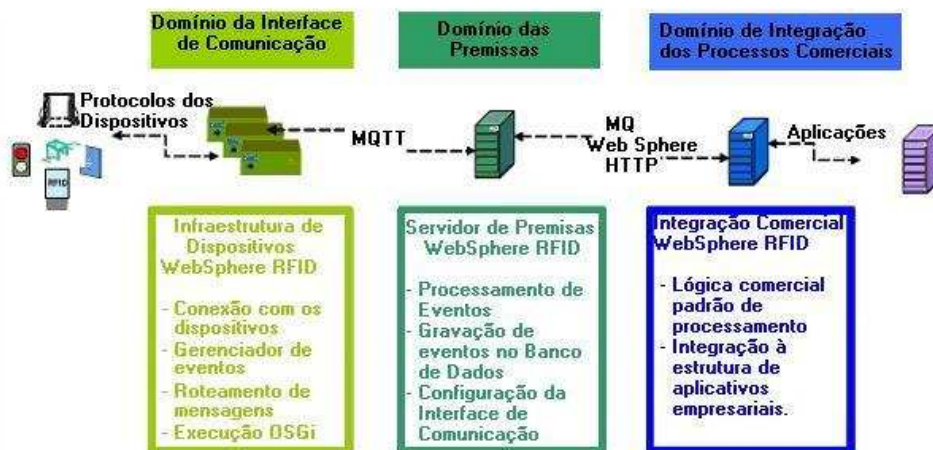



Figura 3.3: Funcionalidades dos componentes.

3.2.1.1 Servidor de Premissas Baseado em WebSphere (*WebSphere Premises Server*)

O WebSphere executa as funcionalidades do domínio das Premissas. Possui dispositivos de processamento de eventos e informações provenientes dos leitores RFID e demais equipamentos do domínio da

Interface de Comunicação (Edge Domain). As saídas desse domínio normalmente são visualizadas pelo domínio de Integração de Processos Comerciais (Business Process Integration Domain) ou, eventualmente, por outros domínios que necessitem de tais informações.

O intenso volume de dados gerados pelos dispositivos RFID deve ser interpretado e analisado para garantir o controle das atividades e dos dispositivos rastreados. Os dados obtidos devem ser processados agilmente e integrados internamente à rede da empresa, compartilhados com as áreas responsáveis e, quando necessário, com parceiros envolvidos no processo.

Assim, percebe-se que este servidor atua como intermediário entre o mundo físico (leitores e tags) e o domínio de integração com a empresa, cujas atividades geralmente são gerenciadas por aplicações de Tecnologia da Informação. Dessa forma, permite dedicação às necessidades específicas da empresa e garante interpretação e integração aos aplicativos de parceiros ou clientes.

As funcionalidades destinadas ao servidor de premissas são:

- Processamento de Eventos - sustenta o alto fluxo de eventos RFID e abriga o ambiente de execução das premissas específicas de cada empresa. Essas premissas definem o tipo de aplicação para atender às demandas específicas.
- Banco de Dados para eventos - todos os eventos reportados ao servidor são armazenados em um banco de dados DB2 (proprietário IBM). Este sistema permite integração com bancos de dados de outros sistemas ou mesmo lógicas de parceiros comerciais e clientes.
- Configuração da Interface de Comunicação - A topologia do domínio de comunicação (Edge Controller) também é definida neste servidor. Os arquivos de configuração são salvos em formato XML devido à flexibilidade conferida por esta linguagem para o compartilhamento de informações através da Internet. Ao iniciar o funcionamento do sistema, estes arquivos são lidos no servidor de premissas e executados no domínio da Interface de comunicação.

3.2.1.2 Infra-estrutura WebSphere do Dispositivo RFID (*WebSphere Device Infrastructure*)

A infra-estrutura do dispositivo é basada em um software que permite um pré-processamento dos dados provenientes do domínio da Interface de Comunicação. Por isso é considerado o centro de processamento da solução IBM. Sua principal característica é a flexibilidade, tão necessária no cenário dinâmico RFID. Como não há ainda padrão para a transmissão de dados RFID, é um desafio para um software trabalhar diretamente ligado à camada física dessa solução.

O software recebe, interpreta e encaminha as informações para o local adequado, de acordo com o *status*. Em caso de erro (necessidade de processamento), a informação é entregue ao servidor de premissas; em caso de aceitação, é agragada junto às demais leituras com status semelhantes. Toda informação obtida pelas leituras deve ser processada, independentemente dos formatos ou do hardware utilizado na obtenção dos dados. Por isso, o software pode ser embarcado em qualquer dispositivo com memória e capacidade de processamento simples, devido ao seu tamanho reduzido e suas funções básicas.

As atribuições desse software não são complexas, se comparadas às funções desempenhadas pelos demais aplicativos da solução IBM, mas são imprescindíveis para o controle do intenso fluxo de dados a

ser manipulado. As características são:

- Independência de dispositivos - a infra-estrutura deve ser transparente, ou seja, as complicadas definições de configuração dos dispositivos, protocolos de comunicação e linguagens privadas dos fabricantes dos equipamentos de leitura não devem ser relevantes para configurar o software. Isso permite que um único ponto de integração das estruturas, por não enxergar as complexidades dos componentes, gerencie múltiplos leitores ou outros dispositivos.

- Sensores de monitoramento - embora os leitores possam operar continuamente, existem fatores que exigem o controle de tais equipamentos, como: restrição (em alguns países) da potência emitida por esses leitores e do período máximo durante o qual os mesmos podem permanecer ligados; prevenção de tráfico desnecessário de informações provenientes das tags em períodos não essenciais; evitável interferência com outros leitores e prolongada exposição de humanos à radiofreqüência.

- Dispositivos de controle de operação - permite controle de mecanismos atuadores tipo mecânicos, que controlam objetos em movimento, como um braço mecânico ou portão automático. Gerencia também dispositivos eletrônicos, como luzes de sinalização para identificar atividades ou displays.

- Filtragem - realiza filtros primários configurados de acordo com as definições estabelecidas no servidor das premissas, para que os dados requisitados pelos processos superiores sejam corretamente selecionados e enviados.

- Agregar dados das tags - cada leitura de um conjunto de produtos poderia ser processada individualmente, mas o fluxo gerado seria constante e intenso. Por isso, é desejável que os dados redundantes provenientes de sucessivas leituras sejam agrupados, para evitar processamento repetido. Isso reduz o tráfego na rede e diminui as tarefas para o servidor das premissas, que pode direcionar seu processamento para outras atividades.

- Gerenciamento remoto das atualizações das distribuições dos softwares - as mudanças constantes nas normas demandam atualizações dos *firmwares* periodicamente para garantir atendimento aos novos padrões. O gerenciamento remoto dos dispositivos acelera os processos e reduz custos para as empresas.

- Desempenho confiável - garantia do processamento de todas as leituras das tags. O modo de operação é assíncrono com o servidor de premissas. Isso permite atuação sem a necessidade de suporte dos sistemas de base, garantindo a capacidade do software operar sem interrupções.

3.2.1.3 WebSphere de Integração Comercial (*WebSphere Business Integration*)

Essa etapa da solução IBM trabalha com a infra-estrutura preexistente na empresa interessada no emprego do sistema RFID. As decisões gerenciais devem ser estudadas caso a caso e configuradas corretamente, para que a conexão e a comunicação RFID seja a mais clara possível.

Permite gerenciar, estruturar e armazenar todo o processo de produção de um equipamento, por exemplo. É possível também basear no histórico armazenado de um produto decisões futuras para fabricação de um equipamento semelhante.

É importante ressaltar que apenas informações provenientes de casos específicos, exceções aos erros comuns e imprevistos chegarão a essa etapa. Por isso, o ambiente aqui desenvolvido é específico para cada empresa e, normalmente, proprietário.

3.3 CONCENTRADOR SAVANT (*SAVANT CONCENTRATOR*)

Esse software foi desenvolvido pelo Auto-ID Center, sediado no Instituto de Tecnologia de Massashussets (MIT). Assim como o *IBM WebSphere RFID Solution*, funciona como middleware, ou seja, conecta o mundo físico RFID (tags e leitoras) e os aplicativos das empresas, com função principal de gerenciamento em ambiente computacional das aplicações possíveis para a tecnologia RFID.

O Auto-ID Center é patrocinado por grandes marcas e lojas, mais interessadas em rastreabilidade e segurança do produto do que na quantidade de informações que podem ser armazenadas em uma tag. Para o desenvolvimento da tecnologia RFID, baseia-se na identificação universal e singular de cada produto - o chamado EPC (Código Eletrônico do Produto). A informação de identificação é codificada em tags de baixo custo, junto a outras características do objeto rastreado. Essas informações podem ser disponibilizadas na Internet, mediante solicitações permitidas. Esse software é muito utilizado devido ao prestígio do laboratório no qual foi desenvolvido e também por ser esse laboratório um dos desenvolvedores dos padrões para a tecnologia. Porém sua ideologia é pouco voltada para a área comercial, mais focada na área de desenvolvimento tecnológico.

O Savant é um concentrador, ou seja, a função principal é agregar as informações. Atua como um redutor de fluxo, com processamento em cada etapa, para garantir o tratamento de todas as informações lidas. Ele captura os dados da leitora RFID, realiza uma filtragem inicial, busca produtos de acordo com as necessidades e envia a informação para os aplicativos da empresa ou para o banco de dados. Feito isso, o concentrador verifica erros e anomalias operacionais e aplica os conceitos definidos para identificar eventos críticos gerenciais. Então envia a informação, já em quantidade menor e tratada, para outra base de dados da empresa, usuário ou ambos. Após o tratamento das informações pelos concentradores, uma estrutura adequada (*pipelines* para destribuição) deve ser desenvolvida para encaminhar os pacotes de dados EPC ou coordenar e processá-los. Para melhor desempenho, mais de um concentrador deve ser empregado em um conjunto de máquinas distribuídas, cada uma controlando um domínio de atividade RFID, como ilustrado na figura 3.4 [13].

3.3.1 Arquitetura da Estrutura de Componentes da Rede EPC

O ambiente proposto pelo Auto-ID Center, baseado nos padrões do EPC Global para desenvolvimento de aplicações RFID é o sistema de comunicação EPC. A arquitetura dos componentes e camadas dessa estrutura são ilustrados na figura 3.5. As camadas e etapas do sistema estão descritas a seguir:

1. Leitores e Sensores

   Para essa camada, o Savant possui um protocolo específico, que define o protocolo padrão da comunicação entre os leitores e o Savant. Também possui um adaptador de protocolo para permitir comunicação com leitores mais antigos, que não implementem o protocolo de leitor Auto-ID.

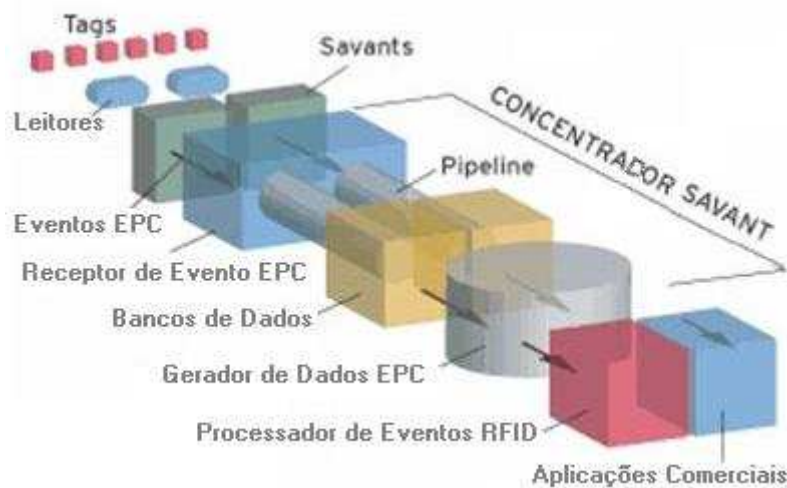



Figura 3.4: Estrutura do Concentrador Savant com *pipelines*

As funções dos leitores e das tags já foram amplamente discutidas nos capítulos anteriores e, por isso, não serão novamente apresentadas. A ênfase foi dada às características específicas desses equipamentos no Savant *Concentrator*.

2. Serviço de Informação EPC (*EPC Information Service*)

   Dados disponíveis pelo serviço de informação EPC podem incluir leituras dos dados armazenados nas tags coletadas pelo Savant, dados de lote de fabricação, como data de fabricação, data de vencimento e também informações do objeto, como as informações de catálogo do produto.

3. ONS - Seviço de Nomeação do Objeto (*Object Name Service*)

   Provê um serviço de busca local que transforma o código EPC em um localizador de referência uniforme de Internet (URLs - *Uniform Reference Locators*). As informações desejadas futuramente de um objeto podem ser buscadas pelos URLs. Usualmente os URLs identificam um sistema de informação EPC, mas o ONS também pode ser usado para associar EPCs com páginas e outras referências da Internet relevantes para o produto.

   Os serviços do ONS podem ser estáticos ou dinâmicos. Serviços estáticos geram URLs tipicamente para informação fornecida pelo fabricante do objeto. Serviços dinâmicos ONS gravam a seqüência de movimentação de um objeto pela linha de fabricação, por exemplo.

4. Cache local ONS (*ONS local cache*)

   É usada para reduzir o número de solicitações ao ONS global para cada objeto rastreado. As informações solicitadas com freqüência e as mais recentes podem ser armazenadas em cache local, que funciona como a primeira chamada para solicitações do tipo ONS.

5. PML (*Physical Markup Language*)

   O PML é uma coleção de vocabulário comum, padrão XML, que representam e distribuem informações relacionadas aos objetos habilitados na rede EPC. Parte do esforço do Auto-ID Center é voltada para desenvolvimento de interfaces padronizadas e protocolos de comunicação internos e externos

Figura 3.5: Componentes e camadas da arquitetura de Rede EPC.

à infra-estrutura Auto-ID. É possível, dessa forma, que haja comunicação direta entre empresas que têm interesses na rastreabilidade dos produtos, figura 3.6.

3.3.2 Visão Geral do Savant

Savant é o software middleware projetado para processar os pacotes de dados (dados de eventos) provenientes de um ou mais dispositivos de leitura. O savant agrega e filtra os dados dos eventos, além de contá-los, para maior controle. Essas funções permitem a redução do volume de dados a ser enviado para os aplicativos da empresa e consomem parte do processamento do Savant. Uma outra parte da capacidade de processamento é destinada às características específicas da arquitetura EPC, como ONS e PML.

Os requisitos do sistema para processamento EPC variam por aplicação. Como o padrão EPC ainda está em desenvolvimento, a ênfase do Savant é em capacidade de extensão, em contraste com a ênfase em características específicas de processamento. Sua organização, ao contrário do concorrente IBM, evita a criação de um único padrão, aplicável a todos os tipos de aplicações. Para permitir utilização por grupos independentes de usuários, a organização é feita em módulos, adequados para o serviço específico de interesse, figura 3.7.

O Savant é um contêiner de módulos que interagem com o mundo externo à esfera RFID através das interfaces definidas: interface do leitor - permite a conexão aos leitores de tag, especialmente, leitores RFID; interface do aplicativo - permite conexão à aplicativos externos como a estrutura da empresa na qual o sistema está inserido, novos aplicativos exclusivos EPC ou outros Savants. No último caso, os softwares devem ser conectados por estruturas de direcionamento de dados (*pipelines*), que distribuam os eventos corretamente para seu próximo processador, de forma que o tratamento de toda informação seja efetuado.

Figura 3.6: Exemplo de comunicação possível entre empresas

Além das duas interfaces definidas pelo Savant, os módulos de processamento componentes podem comunicar-se, através de aplicações (APIs) definidas por eles próprios. Em alguns casos, os módulos de processamento podem comunicar-se com outros serviços externos, através das interfaces definidas por esses serviços. Essa propriedade é o que possibilita a comunicação entre dois sistemas Savant. As APIs, nessa versão do Savant, não definem como os módulos de processamento acessam tais serviços externos. As próximas versões definirão o acesso desses módulos a determinados sistemas externos, como serviço de informação EPC, ONS e outros aplicativos Savant.

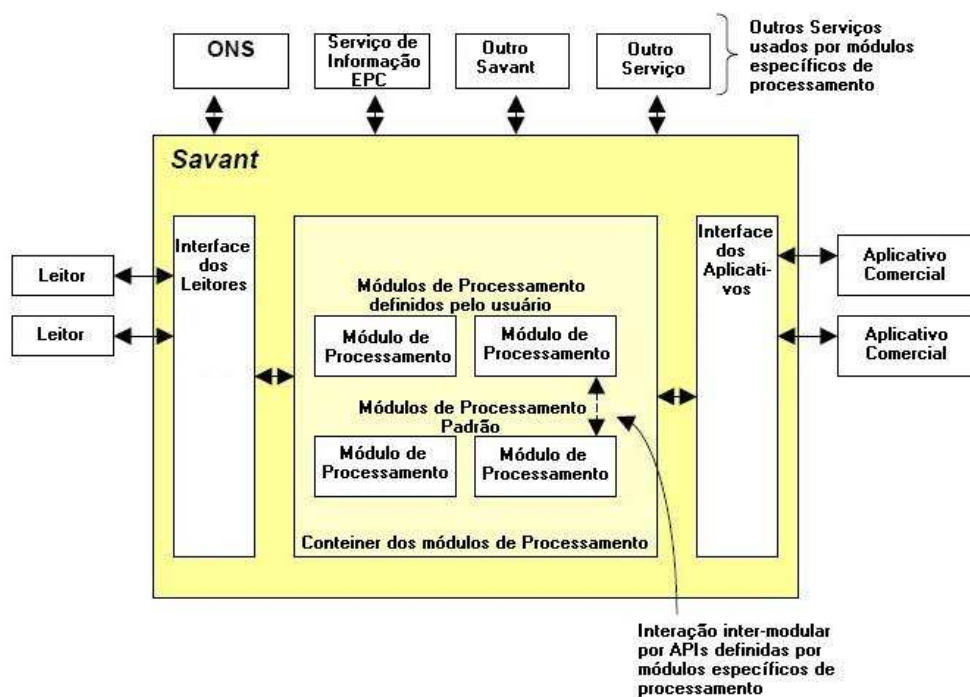



Figura 3.7: Modelo modularizado das interfaces do Savant.

4 PROPOSTA DE UM SISTEMA CONTROLADOR DE FLUXO DE DADOS RFID

4.1 INTRODUÇÃO

Sistemas RFID apresentam incontáveis melhorias relativas aos sistemas anteriores de controle de produtos e máquinas, conforme ilustrado ao longo deste trabalho. O controle real de produtos só é possível ao se tratar as situações e os eventos de real importância, ao invés de todos os dados obtidos.

O sistema IBM, discutido no capítulo 3, apresenta uma solução completa para implantação e utilização de um controlador RFID, possível para várias aplicações distintas, sem necessidade de grandes adaptações. Ele demanda grandes investimentos e disponibilidade de recursos da empresa interessada, o que acaba restringindo sua utilização apenas por grandes empresas, cujos produtos comercializados exigem alta segurança.

O concentrador Savant é uma iniciativa semelhante ao sistema IBM. Não busca clientes, pois o Auto-ID Center, responsável por seu desenvolvimento, é patrocinado por clientes interessados em aplicações particulares. O interesse maior do laboratório é desenvolver e agregar o máximo de funcionalidades à uma mesma aplicação RFID. O concentrador é somente uma ferramenta para permitir evoluções da tecnologia.

Empresas com menores investimentos financeiros para implantação de um sistema RFID necessitam de ferramentas simples e específicas para sua aplicação. O sistema RFID, em todos os casos, gera trânsito de informações elevado o que exige o controle de fluxo. O aplicativo para gerenciamento e tratamento dos dados gerados deve estar, portanto, de acordo com o cenário ao qual se aplica.

Este capítulo apresenta um sistema controlador de fluxo RFID proposto para uma aplicação particular. Também são apresentadas as ferramentas computacionais utilizadas na construção do sistema, o cenário ao qual se aplica, as considerações necessárias para seu desenvolvimento e, finalmente, o fluxograma esquemático de seu funcionamento. As ferramentas utilizadas, as funções existentes e as considerações realizadas são necessárias para permitir uma aproximação mais realista de um sistema RFID completo, pois a aplicação e desenvolvimento restringe-se a simulações.

4.2 FERRAMENTAS COMPUTACIONAIS

4.2.1 JAVA

A linguagem de programação Java, desenvolvida pela SunMicrosystems, foi estabelecida como a linguagem para desenvolvimento do software em função de ser uma linguagem com código aberto. Os modelos preexistentes de controladores estudados também são baseados em JAVA, o que indica que esta linguagem é apropriada para sistemas RFID.

Fontes Java são compiladas em *bytecodes*, que são interpretados pelas Máquinas Virtuais Java (*JVM* -

Java Virtual Machine). Desta forma, os programas Java são independentes de plataforma, executando em qualquer sistema que possua uma JVM.

O ambiente de programação Java é constituído por cinco elementos:

- A linguagem Java;
- As bibliotecas básicas;
- A estrutura dos arquivos .*class*;
- As definições dos bytecodes;
- A especificação da JVM.

Independentemente do desenvolvedor da JVM (Netscape, Microsoft, Borland, etc), ela necessariamente deve respeitar os três últimos itens da lista acima desenvolvido pela Sun.

A Máquina Virtual Java (JVM) é um conceito de software, definindo um computador teórico com um conjunto lógico de instruções, ou **pseudocódigos**, que definem as operações realizadas pelo computador. Em Java, este pseudocódigo é formado por bytecodes.

Os bytecodes são, em geral, executados por um outro programa, o interpretador Java. O interpretador Java entende o conjunto lógico de instruções representado pelos bytecodes, simulando a arquitetura virtual para a qual foram desenvolvidos. Além de executar uma JVM, o interpretador ainda fornece um ambiente de execução, com garbage collector para o gerenciamento de memória e a funcionalidade necessária para acessar arquivos .class [14].

A estrutura básica de um aplicativo Java é composta por um bloco de instruções **import** e um bloco de declaração da classe do aplicativo. A classe, assim como seus métodos, são delimitados por chaves ({}).

1. Declaração do Pacote **package**

   Os pacotes são mecanismos para agrupamento das classes. Nele são colocados as variáveis e os métodos da classe. Portanto, toda classe pertence à um pacote. A declaração **package** precisa ser a primeira linha não comentada em um arquivo. O trecho do código do software desenvolvido na figura 4.1 exemplifica a declaração de pacotes.

```
1 package controle_estoque;
2
3 public class Password {
4
5     public String getPassword(String campo, String usuario){
```

   Figura 4.1: Declaração de pacote no desenvolvimento do software

2. Bloco de Instrução **import**

   O Kit de Desenvolvimento Java (JDK - *Java Development Kit*) oferece um imenso conjunto de classes que estão agrupadas em pacotes para criação de aplicativos. Importando esses pacotes podemos

utilizar todas as variáveis e métodos das classes Java, reduzindo dessa forma a quantidade de linhas de código que seriam necessárias para executar tarefas. Para utilizar um método pré-definido, basta importar o pacote correspondente, como por exemplo *java.awt*, ou apenas uma das classes do pacote, como *javax.text.DecimalFormat*. No código do software, foram importados alguns pacotes e classes, figura 4.2.

```
1  package controle_estoque;
2
3  import java.awt.*;
4  import java.awt.event.*;
5  import java.io.IOException;
6  import java.net.URL;
7  import java.text.DecimalFormat;
8
9  import javax.swing.*;
10
11 import com.mysql.jdbc.exceptions.MySQLSyntaxErrorException;
12
13 public class InterfaceInicial extends JFrame {
14
```

Figura 4.2: Bloco de instrução para importar pacotes e classes

3. Declaração de Variáveis

   A declaração de variáveis segue o formato <tipo> <nome da variável> (<atributo>), como por exemplo **int i = 0**. O atributo só é necessário se a variável for declarada dentro de um método. Caso seja uma variável da classe, não necessita ser inicializada.

   Além disso, pode-se utilizar um dos modificadores de acesso: *public*, *private* ou *protected*. O modificador *public* torna uma variável acessível por qualquer classe ou método. O modificador *private* indica que a variável não está disponível para qualquer outra classe ou método, com exceção daqueles aos quais ela pertence. O modificador *protected* restringe o acesso apenas às subclasses. O uso de variáveis dentro de classe e método está mostrado no trecho de código da figura 4.3.

```
7  public class GerarRelatorio {
8
9      private String linhaRelatorio;
10     private String[] arrayDeIds, arrayDePrecos;
11
12     private void escrita(String tabela, String data, int quantidadeDados, int qualEscrita, double saldo){
13
14         FileOutputStream fos = null;
15         OutputStreamWriter osw = null;
16         BufferedWriter bw = null;
17         int countArrayId = 0;
```

Figura 4.3: Declaração de variáveis de classe e variáveis de método

4. Declaração de Métodos e Classes

   Os módulos de um programa Java são chamados de métodos e classes. As definições de classes de java normalmente contêm um ou mais métodos. Para as classes de um aplicativo Java, um dos métodos deve ser chamar **main**, pois é a partir desse método que começa a execução do programa.

Os métodos podem ou não retornar informações quando finalizam suas tarefas. A palavra-chave **void** indica que o método realizará sua tarefa e não retornará nenhuma informação. Exemplos de métodos são mostrados no trecho de código da figura 4.4.

```
5   public void setEstoque(String id, String preco, String fabricante, String produto){
6       String sql = "INSERT INTO Estoque VALUES('"+ id + "', 'Estocado', CURDATE(), '"+
7       preco + "', '"+ fabricante + "', '" + produto + "')";
8       BancoDeDados.setIntoTable(sql);
9   }
10
11  public String getEstoque(){
12      String sql = "SELECT * FROM Estoque";
13      String estoque = BancoDeDados.getTable(sql, "*");
14      return estoque;
15  }
16
```

Figura 4.4: Métodos que retornam e não retornam informação

O Java é uma linguagem orientada a objetos, distribuída, que permite múltiplas linhas de execução, além de ser dinâmica, portável, robusta, neutra, segura e simples [15]. Essas características fazem com que a linguagem permita algumas vantagens em relação às demais:

- Facilidade de Manutenção

  O fato de Java ser fortemente orientada a objetos, faz com que seja possível desenvolver componentes que podem ser incorporados em aplicações de banco de dados. Sua hierarquização é facilitada no sentido de manter os componentes organizados.

- Conectividade

  A linguagem Java incentivou o desenvolvimento de vários softwares de conectividade de banco de dados. Existe uma variedade de bibliotecas para bancos de dados (APIs) disponíveis para Java e de dispositivos que utilizam JDBC (Interface de conectividade Java - Banco de Dados). É possível, portanto, desenvolver aplicações comuns e industriais (applets) que se comunicam com vários tipos de servidores de bancos de dados [16].

- Consistência

  A API JDBC possibilita o desenvolvimento de applets e aplicações Java independentes de bancos de dados. Com essa biblioteca de conectividade é possível se construir aplicações portáveis para uma grande variedade de servidores de bancos de dados.

- Facilidade de Prototipação

  A linguagem Java permite a reutilização de componentes já implementados por outros desenvolvedores, o que agiliza o processo de criação de um protótipo com interface gráfica.

Para o desenvolvimento do software foi utilizado o Java Standard Edition por ser a versão da linguagem Java indicada para desenvolvimento de aplicações de pequeno porte. Nessa seção, foi apresentado alguns blocos de código do software que foi desenvolvido. Os diagramas de blocos representando a interelação das classes são apresentados no anexo I.

4.2.2 IDE Eclipse

Uma IDE (*Integrated Development Environment*) é o ambiente de desenvolvimento integrado da linguagem de programação. É um programa editor, utilizado para facilitar a geração do código e futuras correções. Os programas Java dividem-se normalmente em cinco fases a serem executadas, figura 4.5.

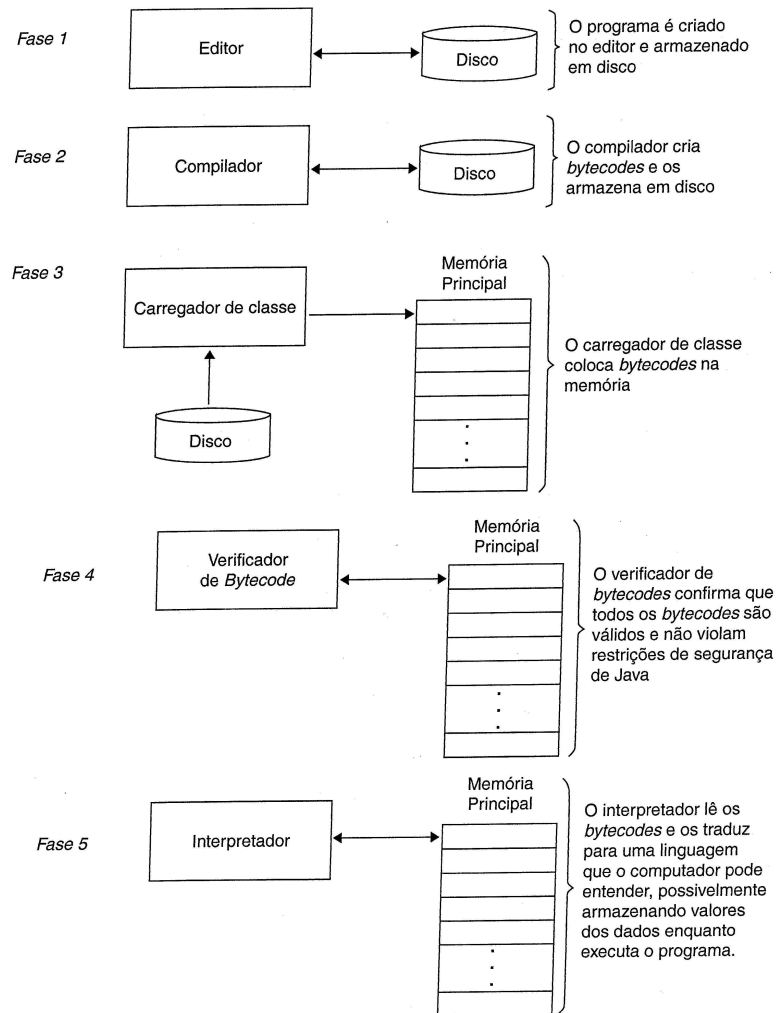



Figura 4.5: Fases do processo de criação de um programa em Java.

- Fase 1 - Criação e Edição

  Consiste em criar e editar um arquivo, normalmente realizado por uma IDE. Esse arquivo, que normalmente possui a extensão do tipo **.java**, contém o programa a ser executado.

- Fase 2 - Compilação

  Consiste em compilar o programa gerado. Caso não haja falhas no código, o compilador traduz o programa para *bytecodes*, ou linguagem de máquina. São gerados então arquivos do tipo **.class**, contendo os *bytecodes* que serão utilizados durante a execução do programa.

- Fase 3 - Carga

Para ser executado, o programa deve ser colocado na memória. Essa tarefa é realizada pelo carregador de classe, que pega os arquivos **.class** contendo *bytecodes* e os transfere ou para a memória do computador local (aplicativos - uso local) ou para um computador remoto, que usuários conectam via Internet (applets - uso industrial). Para acessar um applet novamente, o usuário deve apontar seu navegador para a localização na Internet e carregar o programa no navegador. Para acessar um aplicativo, o usuário pode simplesmente cliquar sobre o ícone e executá-lo, se estiver utilizando sistemas operacionais como Windows ou Linux.

- Fase 4 - Verificação

  Os *bytecodes* são verificados por um verificador de *bytecode* antes de um applet ser executado pelo navegador ou antes de um aplicativo descarregar *bytecodes* de uma rede. Isso assegura que os bytecodes, para classes carregadas a partir da Internet, são válidos e não violam as restrições de segurança de Java. Essa funcionalidade faz com que o Java seja uma linguagem segura, pois impede que programas descarregados pela rede causem danos aos seus arquivos e seu sistema.

- Fase 5 - Interpretação

  O computador, sob o controle da CPU, interpreta o programa, um *bytecode* por vez, realizando a ação especificada pelo programa. Cabe ressaltar que o processo descrito pelas cinco fazes deve ser dinâmico e iterativo, ou seja, se ao chegar a fase final, um erro de lógica ou uma falha de execução for encontrada, deve-se retomar à fase 1, repetindo todo o processo.

A IDE escolhida para o desenvolvimento do software foi o Eclipse, figura 4.6. Esse editor automaticamente realiza as funções descritas pelas fases 2 a 5 (compilação, carga e verificação) quando o programador salva seu código localmente. Ele permite também a execução local do programa, dentro do próprio editor. Assim, é possível identificar falhas no processo de criação do código e erros de lógica ou sintaxe, sem necessidade de finalização do código para futuros testes e identificação de erros.

O Eclipse é um programa *freeware*, ou seja, pode ser utilizado para fins não comerciais sem custos, além de ser um programa que demanda pouco espaço em disco, pois não necessita de instalação.

4.2.3 MySQL

O My SQL é um sistema de gerenciamento de banco de dados que utiliza a linguagem SQL (*Structured Query Language* - Linguagem de Consulta Estruturada) como interface. É um dos bancos de daods mais populares, com mais de 10 milhões de instalações pelo mundo.

Suas principais características são: portabilidade, pois suporta grande variedade de pltaforfmas; compatibilidade com a linguagem JDBC que realiza a interface para JAVA; excelente desempenho e estabilidade; pouco exigente quanto a recursos de hardware e facilidade de uso.

Esse sistema é reconhecido pelo seu desempenho e robustez, e por realizar várias atividades simultaneamente, podendo ser acessado por vários usuários. Considerado um sistema mais leve com aplicações pouco exigentes, acaba sendo preterido por outros sistemas. É um software livre, com suporte a tabelas de tipos específicos para cada finalidade. Outra grande vantagem é a de ter código aberto e funcionar em um grande número de sistemas operacionais, como Windows, Linux, FreeBSD, BSDI, Solaris, Mac OS X, SunOS, SGI.

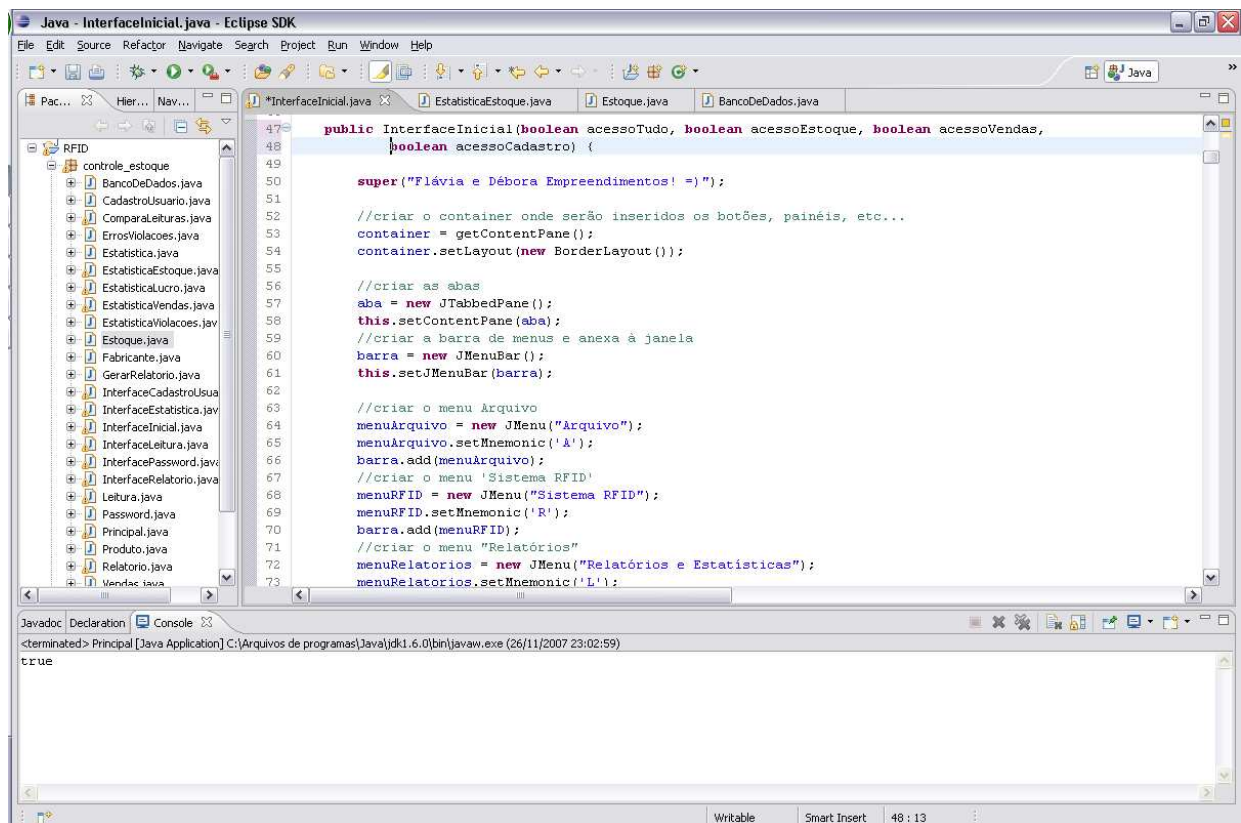



Figura 4.6: Exemplo da IDE Eclipse

4.3 CENÁRIO

O cenário imaginado para a implantação do software proposto é uma livraria de pequeno porte. Todos os livros dessa empresa recebem uma etiqueta RFID contendo informações sobre cada exemplar. Um código serial único é associado a cada exemplar, de forma que a rastreabilidade de cada item seja possível.

A estrutura de hardware da loja para a implantação desse sistema contém: uma unidade central que atua como servidor e banco de dados onde os dados são armazenados; terminais de vendas conectados diretamente ao servidor e, finalmente, uma unidade de controle destinada à solução dos eventos RFID, ligada diretemente à estrutura de segurança da loja.

A livraria deve ter uma área que garanta a capacidade de leitura dos produtos no interior da loja com apenas um dispositivo leitor. Considera-se também que não haja leitura de livros do exterior da loja, possívelmente já vendidos. A figura 4.7 ilustra a disposição da empresa.

As etapas de um sistema RFID para controle de estoque da livraria pode ser descrito pela figura 4.8. O sistema proposto é um middleware, ou seja, é o intermediário entre as estruturas de hardware, como tags, leitoras e sinalizadores de violações de algum item em estoque.

Os componentes físicos, tais como etiquetas, leitores, estruturas de comunicação entre os dispositivos e as unidades de processamento, necessários para implantação do sistema real RFID não estavam disponíveis no ambiente acadêmico onde foi desenvolvido este software controlador. Isso impediu a realização de testes do software proposto atuando diretamente no sistema para o qual foi projetado.

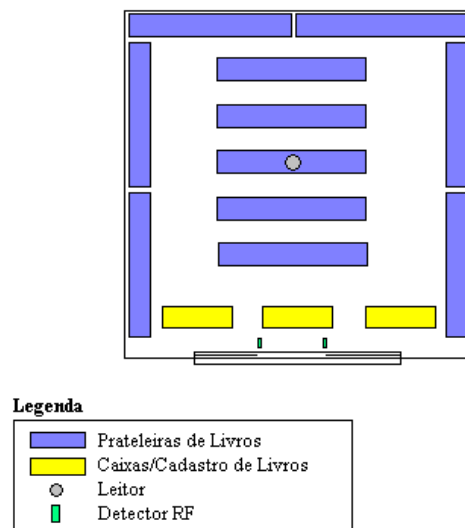



Figura 4.7: Disposição da livraria.

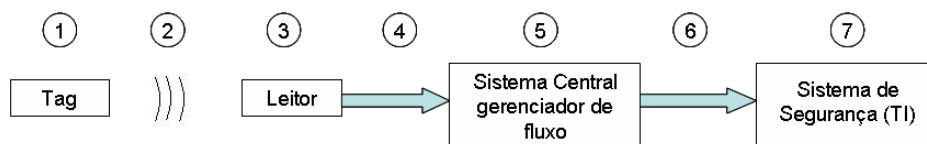



Figura 4.8: Fluxo de Dados em um sistema RFID de controle de estoque.

Para simular uma efetiva comunicação de dados entre as unidades componentes do sistema RFID e realizar testes do sistema controlador de fluxo desenvolvido, algumas considerações são feitas. A figura 4.8 é utilizada como referência para a descrição das considerações:

1. Tags

   As tags são capazes de armazenar todos os dados de cadastro dos livros. São gravadas e impressas na livraria, vinculadas ao cadastro de estoque. A figura 4.9 ilustra uma impressora de tags RFID, que pode ser usada pela empresa.

2. Comunicação entre tags e leitor

   Considera-se, para teste do software proposto, que todas as tags são sempre lidas pelos leitores. Assim, os livros que pertencem ao estoque e que não constam como vendidos são tratados como violados. Essa comunicação por radiofreqüência é a grande vantagem do sistema RFID em relação ao usual código de barras. A tecnologia de código de barras demanda funcionários manuseando leitores de códigos de barras para realizar leitura individual de cada item. O leitor deve estar ligado por cabo à um computador, conectado em rede ao sistema central. Esse deve conter todos os livros em estoque. O procedimento de leitura dos itens, por ser lento e físico, normalmente é realizado ao final do dia e só então, os dados de estoque final podem ser confrontados com os de estoque inicial e vendas, para controle de possíveis violações. O sistema RFID permite controle mais intenso dos livros, já que periodicamente são realizadas leituras comparativas de estoque. Essas leituras não demandam pessoal ou instrumentos físicos que atrapalham circulação de clientes pela loja, pois o

Figura 4.9: Impressora de tags RFID.

leitor fica posicionado no teto da loja. Em espaço de minutos (intervalo entre leituras consecutivas) é possível identificar violações e, caso haja um circuito interno de filmagem, é possível imediatamente identificar o sujeito da infração.

3. Leitores

   Esses dispositivos possuem memória interna pequena, além de microprocessadores acoplados, o que permite que dados provenientes de sucessivas leituras sejam agregados e armazenados localmente. Somente os eventos discrepantes entre leituras sucessivas são transmitidos diretamente para o servidor pela rede interna de comunicação, em caso de aplicativos pequenos, como é o caso do cenário envolvido. Poucos eventos, quando comparado à quantidade de produtos existentes na empresa, serão discrepantes, o que permite que a rede não seja sobrecarregada.

   O software proposto simula a funcionalidade dos leitores: realiza as leituras quando solicitado e a compara com os dados, para seguinte encaminhamento dos eventos discrepantes para o servidor (Sistema Central). É necessário enfatizar que essa é somente uma adaptação do software para permitir a simulação de um cenário RFID real. Na prática, leituras devem ser armazenadas nos dispositivos de leitura para evitar trânsito desnecessário de informações na rede e poupar memória do servidor de banco de dados para outras necessidades.

4. Comunicação entre leitor e o Sistema Central

   O leitor é conectado diretamente ao Sistema Central (servidor), por um cabo, dedicado à essa comunicação. Todos os dados de itens que constam em uma primeira leitura e não constam na leitura consecutiva são necessariamente encaminhados para o servidor e sempre são recebidos. O software solicira então a comparação com a tabela de vendas, também armazenada no servidor. Caso o item não conste nessa tabela, ele será dado como violado e encaminhado pelo sistema central controlador de fluxo para a central de segurança. O fluxo de dados nessa etapa já é consideravelmente inferior aquele da comunicação entre tags e leitor, pois apenas itens vendidos ou violados serão encaminha-

dos.

5. Sistema Central

   O software controlador de fluxo proposto tem como função principal atuar nesse sistema central, gerenciando tabelas de estoque inicial, leituras, vendas, violações e armazenar registros. Ele define as ações de cada etapa do processo de leitura do sistema RFID. É composto por um servidor, que comporte a base de dados e o sistema gerenciador de fluxo.

   O software possui uma interface gráfica para organizar os cadastros necessários para o controle do sistema RFID. Comunica-se com o banco de dados, gerando as tabelas e relatórios para controle, o que evita entrada direta no banco de dados. No capítulo 5, mostra-se detalhadamente o manual de funcionamento do software.

6. Comunicação entre o Sistema Central e o Sistema de Segurança

   Essa comunicação ocorre pela rede interna da empresa, pois são eventos raros. Somente os dados de livros violados são encaminhados para o sistema de segurança. Isso faz com que a rede não seja congestionada, permitindo que os caixas acessem sem dificuldades o servidor, para registros das vendas e que os demais computadores conectados pela rede acessem os dados de interesse, sem falhas de comunicação.

7. Sistema de Segurança

   O sistema de segurança é definido pela empresa, normalmente pela área de Tecnologia da Informação (TI), que define o tratamento de dados. Esse sistema também é representado no software proposto. A empresa pode definir quais os procedimentos para alerta da situação, como por exemplo, disparo de alarme, luz de emergência, alerta dos seguranças da loja.

4.4 FLUXOGRAMA

O software é um controlador de fluxo, mas também permite operações usualmente realizadas por uma empresa. Ele pode ser subdividido em três principais eixos, cada um com funções específicas, figura 4.10:

1. Cadastro - Tem por objetivo informar ao sistema o produto a ser rastreado e as características pertencentes a cada item. Como o software é desenvolvido para uma livraria, a principal função é armazenar dados cadastrais dos itens no sistema e imprimir uma tag contendo as mesmas informações e armazená-la em cada exemplar, de forma que todos os produtos internos da loja possam ser rastreados.

2. RFID - Em um sistema real essa função é desempenhada pelo software embarcado no leitor. Para teste de funcionamento do software proposto, as leituras são simuladas pelo próprio software, através de realização de cópias das tabelas de estoque, sendo possível inserir manualmente violações em exemplares específicos em uma das leituras, sem alterar o estoque. Assim, o sistema compreende a diferença entre as leituras consecutivas como uma possível violação. Devido à essa adaptação do software, pode-se visualizar o processo de controle e rastreabilidade completo, da forma que ele deve se comportar no caso de uma violação real de um componente do sistema.

3. Consolidação - Essa etapa lida com os dados provenientes do sistema como um todo. Consolida dados do estoque, do cadastro, das leituras e realiza busca no banco de dados, para informar, através de relatórios, informações mais claras e de fácil interpretação. Permite também manutenção do sistema, com alterações de preços dos produtos, dados cadastrais de editoras, além de consultas ao cadastro.

O capítulo 5 apresenta as funções do software detalhadamente, com seu manual de instruções e exemplos de funcionamento.

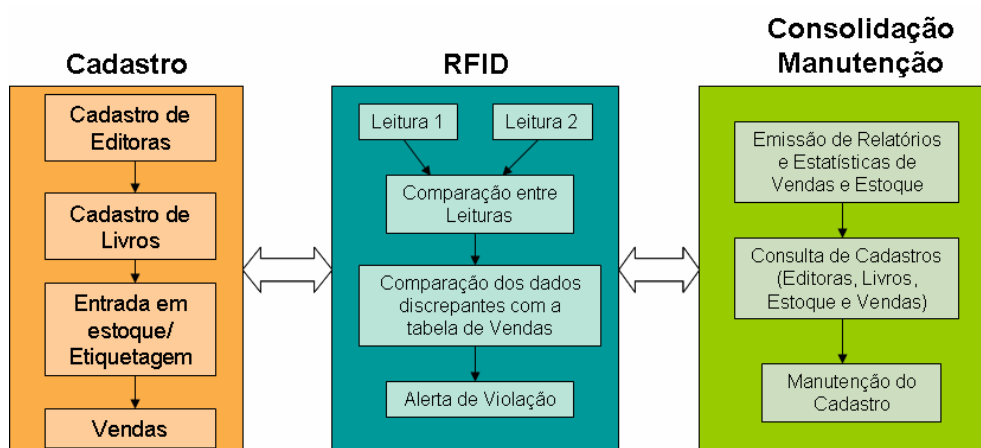



Figura 4.10: Fluxograma dos dados no software proposto.

5 MANUAL DO SISTEMA PROPOSTO

5.1 INTRODUÇÃO

Este capítulo apresenta um manual de funcionamento da versão 1.0 do software proposto, que é voltado para gerenciamento interno, com segurança, dos produtos existentes na loja. Ele apresenta as funcionalidades de sistemas comuns, como, por exemplo, cadastro de fornecedores (editoras), cadastro de produtos (livros) e entrada em estoque, com fixação de etiquetas RFID. A parte de controle RFID é simulada computacionalmente para teste do funcionamento do sistema completo. É possível contabilizar vendas e controlar estatisticamente o desempenho da loja. Para agregar os dados gerais do estabelecimento, o sistema oferece também emissão de relatórios.

5.2 INSTALAÇÃO

A instalação do software proposto consiste na aquisição e instalação das ferramentas necessárias para o funcionamento do sistema além da aquisição dos arquivos **.class** do software e do arquivo **rfid.bat**, responsável por rodar o software. Todas essas ferramentas encontram-se no CD de instalação do programa, no anexo II.

Inicialmente, deve-se fazer a instalação do software de banco de dados MySQL, pelo arquivo **Setup.exe**, que se encontra na pasta **MySQL**. Caso o computador do usuário tenha ou teve uma versão do MySQL instalada, ele deverá desinstalar essa versão e remover a pasta **C:\Arquivos de programas\MySQL**. Feito isso, a instalação poderá ser iniciada.

As telas de instalação guiam o processo. Na primeira tela, deve-se clicar em **Next>**; na próxima tela, seleciona-se instalção Típica **- Typical** e então deve-se clicar no botão **Next>**; pressiona-se **Install** na tela seguinte e então deve-se aguardar a conclusão do processo. Nas duas próximas tela deve-se somente pressionar **Next>** e na última tela marcar a caixa **Configure the MySQL Server now** e então clicar em **Finish**.

A configuração deve seguir o padrão predeterminado para que não ocorra conflito de comunicação no sistema. A primeira tela de configuração deve ser seguida, pressionando-se **Next>**. Na segunda tela de configuração, deve-se selecionar **Standard Configuration** e então pressionar **Next>**. Na próxima tela deve-se checar a caixa **Install as a Windows Service**; o campo **Service Name:** deve estar preenchido com **MySQL** e a caixa **Launch the MySQL Server automatically** deve ser marcada para então selecionar em **Next>**, figura 5.1.

A próxima tela define as configurações para habilitaçao de comunicação do software com o banco de dados. Os campos devem ser preenchidos com as informações:

- o usuário (*User Name*) da conexão será **root**;
- a senha (*Password*) do usuário tem que ser **1234**.

Figura 5.1: Tela de configuração do MySQL.

O campo **Enable root access from remote machines** e **Create an Anonymous Account** devem estar desabilitados. Após preenchido todos os campos, deve-se clicar em **Next>**, figura 5.2.

Na tela final deve-se apenas clicar em **Execute**.

Em seguida, no CD do software deve-se abrir a pasta chamada "'**Java** e instalar o programa **jre-6u3-windows-j586-p.exe**. Aguarde a finalizaçao dessa instalação que atualizará a Java Virtual Machine.

Feito isso, deve-se abra a pasta **Java-MySQL Conector** também no CD, selecionar a pasta chamada **Java** e copiar para o diretório **C:**\. Após essa operação, dentro dessa mesma pasta **Java-MySQL Conector**, deve-se executar o arquivo **instalador.bat**, com clique duplo. Esse arquivo deverá, obrigatoriamente, ser executado apenas uma vez, pois ele cria o banco de dados e as tabelas necessárias para a utilização do software.

Finalmente, deve-se copiar do CD a pasta chamada **RFID** e colar no diretório **C:**\. Essa pasta contém os arquivos para execução do software. Eles estão são bytecodes (**.class**) e estão inacessíveis. Para executar o programa, deve-se sempre executar o arquivo **rfid.bat** da pasta RFID. Esse arquivo não pode ser movido dessa pasta devido às suas referências.

5.3 INICIALIZAÇÃO

Para incializar o programa deve-se abrir a pasta **RFID** no diretório **C:**\ de seu computador.

O software, ao ser instalado, cria automaticamente um usuário, que tem permissão de acesso a todas as funcionalidades do sistema. O nome de usuário padrão criado pelo sistema é **MASTER** e a senha é **1234**.

Figura 5.2: Tela de configuração da senha de acesso ao MySQL

Ao iniciar o software pela primeira vez, é necessário inserir esses dados nos campos da tela de permissão de acesso, ilustrada na figura 5.3, e clicar em **OK**. Nos acessos posteriores é indicado que se utilize as senhas de usuários cadastradas, para evitar acessos indevidos.

Figura 5.3: Tela de permissão de acesso.

A tela principal do programa deve ser então inicializada, como ilustrado na figura 5.4 (a). A primeira atividade a ser desenvolvida é o cadastro dos usuários. Clique em **Arquivo** e, a seguir, em **Cadastrar Usuário**.

Nessa etapa ocorre a definição dos privilégios de acesso ao sistema a ser dado a cada um dos funcionários que utilizarão o sistema, através da tela mostrada na figura 5.4 (b). Caso ocorram erros durante o cadastro, o software alerta o usuário por meio de mensagem de erro. No caso de conclusão do cadastro, há uma mensagem de confirmação.

5.4 CADASTRO/CONSULTA DE FABRICANTES

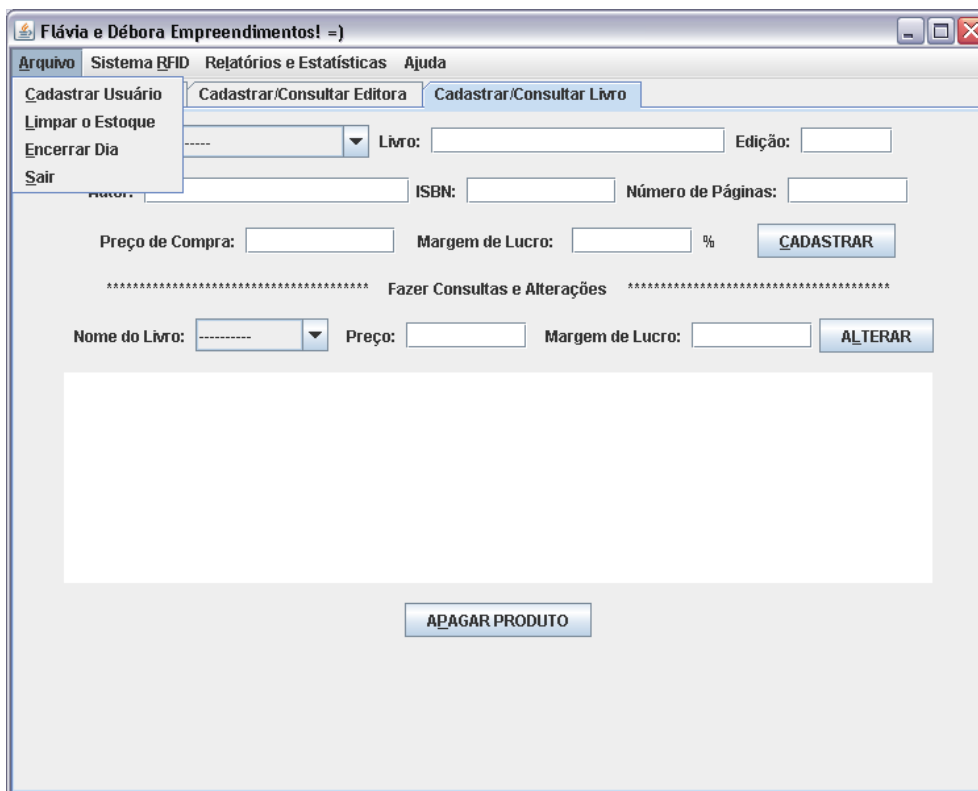
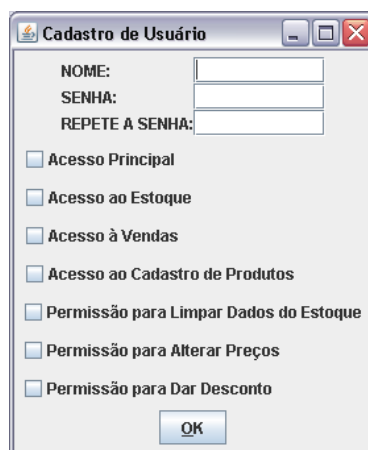
O funcionário com permissão para realização dessa atividade deve cadastrar as editoras que serão fornecedoras dos livros a serem comercializados. Devem ser informados: nome, endereço, telefone, pessoa

(a) Tela principal do software.

(b) Permissões para os usuários.

Figura 5.4: Utilitários de cadastro de usuários.

para contato na editora e e-mail. Esse cadastro é utilizado para referência em caso de necessidade de futuros contatos com a editora. Nessa tela é possível também realizar a consulta dos dados das editoras existentes no cadastro. A figura 5.5 ilustra as funções descritas. Para sair do software, o usuário deve seguir por **Arquivo>Sair**. O botão fechar no topo da tela está desabilitado.

Figura 5.5: Tela de cadastro e consulta de editoras.

5.5 CADASTRO DE PRODUTOS

Na tela ilustrada pela figura 5.6 deve-se realizar o cadastro dos livros a serem comercializados na loja. Somente os usuários com permissão cadastrada no sistema poderão realizar essa atividade. O livro é associado à editora de origem, portanto só pode ser inserido após o cadastro prévio da editora. Todos os campos referentes ao livro devem ser cadastrados. O campo preço de compra refere-se ao preço de aquisição do produto, ou seja, o valor cobrado pela editora por exemplar de cada livro adquirido pela livraria. Ele deve usar ponto '.' como separador de casas decimais. Em caso de uso de vírgula, uma mensagem de erro será mostrada. A margem de lucro é utilizada para cálculo do preço de venda a ser associado ao livro.

É possível, a qualquer momento, consultar os livros cadastrados e alterar os campos preço e margem de lucro. Assim, caso a editora altere os preços de venda de um produto, é possível alterar os dados no cadastro. É possível também alterar margens de lucro, para caso de promoções ou reajustes de preço. Para sair do software, o usuário deve seguir por **Arquivo>Sair**. O botão fechar no topo da tela está desabilitado.

5.6 ENTRADA EM ESTOQUE

A entrada em estoque é realizada ao se informar a quantidade de exemplares de um mesmo livroque serão estocados. Para isso, deve-se informar a quantidade de exemplares, a editora fornecedora e o livro a ser estocado, conforme a figura 5.7. Um número serial único é associado a cada um dos livros a ser estocado. Esse número e os dados de cadastro do livro são armazenados em tags RFID, que são colados na

(a) Tela de consulta e cadastro de livros

Figura 5.6: Tela de consulta e cadastro de livros.

contracapa dos livros. Na parte superior das etiquetas RFID estão impressos os campos ISBN, número de identificação (ID) e um código de barras contendo essa informação. São auto-adesivas e se danificam se removidas, para maior segurança. Essas etiquetas permitem o controle de estoque pelo sistema RFID. Para sair do software, o usuário deve seguir por **Arquivo>Sair**. O botão fechar no topo da tela está desabilitado.

5.7 CONTROLE DE VENDAS

Para realizar uma venda, o funcionário responsável por essa atividade deve aproximar os livros selecionados pelo cliente a um leitor RFID. Esse leitor tem função semelhante à do leitor de códigos de barras, comum hoje em lojas de venda. Isso permite que estabelecimentos que já possuem a infra-estrutura não necessitem de novos investimentos, para obtenção de leitores RFID, pois a etiqueta RFID também possui um código de barras impresso. Assim, a identificação do produto ocorre sem a necessidade de entrada manual de dados. Isso agiliza o processo de vendas e qualifica o serviço oferecido.

O campo denominado **ID** na figura 5.8 (a) é preenchido automaticamente por um leitor e o funcionário pressiona **VENDER**. Caso haja erro de leitura pelo dispositivo eletrônico, é possível inserir manualmente esse campo. No software proposto, a identificação do livro a ser vendido é feita manualmente, devido a inexistência do hardware indicado. O campo deve ser preenchido com todos os caracteres de cadastro. Caso o formato não seja obedecido, um alerta solicita o preenchimento correto, figura 5.8 (b).

Os dados do livro vendido são apresentados pela tabela de vendas, para conferência com o exemplar.

Figura 5.7: Tela de cadastro de estoque.

Caso ele não coincida com os dados apresentados ou haja erro de leitura no ato da venda, é possível excluir itens da venda do cliente. Para isso, no campo **Excluir item da venda**, deve-se digitar o ID do exemplar incorreto que consta como vendido e clicar em **EXCLUIR**. Essa alteração só pode ser realizada por funcionários com permissão específica para tal atividade, o que é confirmado pela exigência de nome de usuário e senha para autorizar o acesso, como ilustrado na figura 5.3.

Quando todos os livros selecionados por um cliente constarem na seleção de vendas, o campo **Valor da Venda** mostra o valor total para cobrança. Após o recebimento da compra, o funcionário deve pressionar **Finalizar Venda**. A partir desse momento, os livros não constam mais em estoque e passam a pertencer ao banco de dados de vendas. Ocorre a desmagnetização da tag, para que o produto não seja detectado pelo dispositivo anti-furto existente na saída da loja, que aciona um alarme em caso de detecção de etiqueta ainda magnetizada. Esse procedimento também evita que um livro já vendido seja novamente detectado pelo leitor do estoque, gerando conflito de informações. Para sair do software, o usuário deve seguir por **Arquivo>Sair**. O botão fechar no topo da tela está desabilitado.

5.8 SISTEMA RFID

O sistema RFID é controlado pela área de segurança, mas pode ser acionado por todos os funcionários a qualquer momento, em caso de suspeitas de violações ou furtos. Ele aparece no menu principal do software, como mostra a figura 5.9 (a).

O sistema RFID real realiza automaticamente leituras periódicas de todas as tags existentes no interior

(a) Tela de vendas.

(b) Alerta de preenchimento incorreto do campo ID.

Figura 5.8: Utilitários de vendas.

da loja, armazena em tabelas no próprio leitor (sistema embarcado) e as compara consecutivamente. Livros que constam em estoque em uma leitura, mas não constam na seguinte são considerados conflito, ou seja, possíveis violações. Assim, somente os conflitos são enviados ao servidor, para comparação à tabela de venda. No servidor o software confere se, no espaço de tempo entre as leituras, o exemplar foi vendido. Em caso positivo, o sistema desconsidera a hipótese de furto, mantendo o registro do conflito. Caso os itens conflitantes não constem também na tabela de vendas, o sistema interpreta como furto e ativa alertas de violação, como o exemplo da figura 5.9 (b).

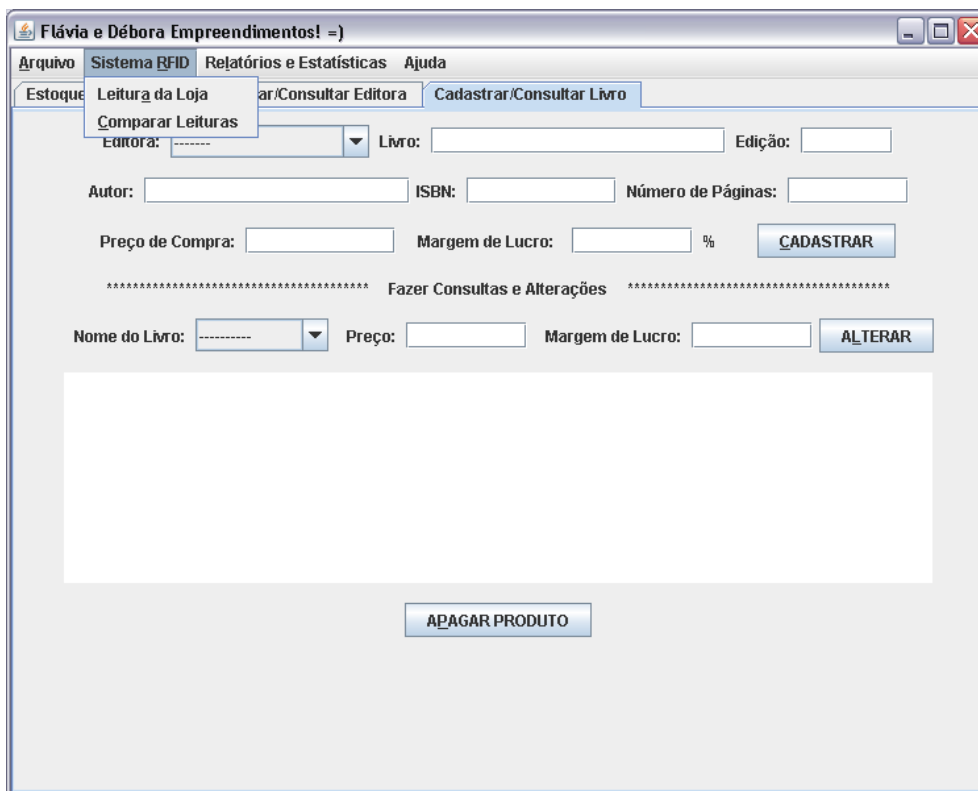
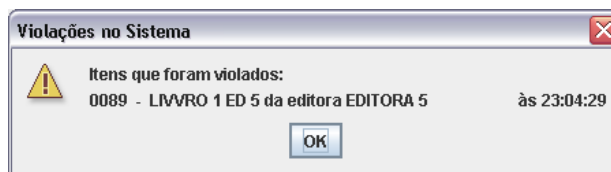
Como no ambiente de desenvolvimento desse projeto não havia disponibilidade de um sistema RFID real, realiza-se uma adaptação para simular leituras e possíveis violações. É importante ressaltar que essas tarefas, em sistemas reais, são realizadas pelo software embarcado no leitor, com armazenamento das tabelas no próprio equipamento. Somente o tratamento de dados, aqui descrito pela comparação com a tabela de vendas e alerta de violação, é realizado pelo sistema da loja. Abaixo estão os passos para simulação de leituras e violações:

(a) Sistema RFID.

(b) Alerta de Violação

Figura 5.9: Utilitários do Sistema RFID.

1. Clicar em **Sistema RFID** no menu da tela principal, ilustrado na figura 5.9 (a).

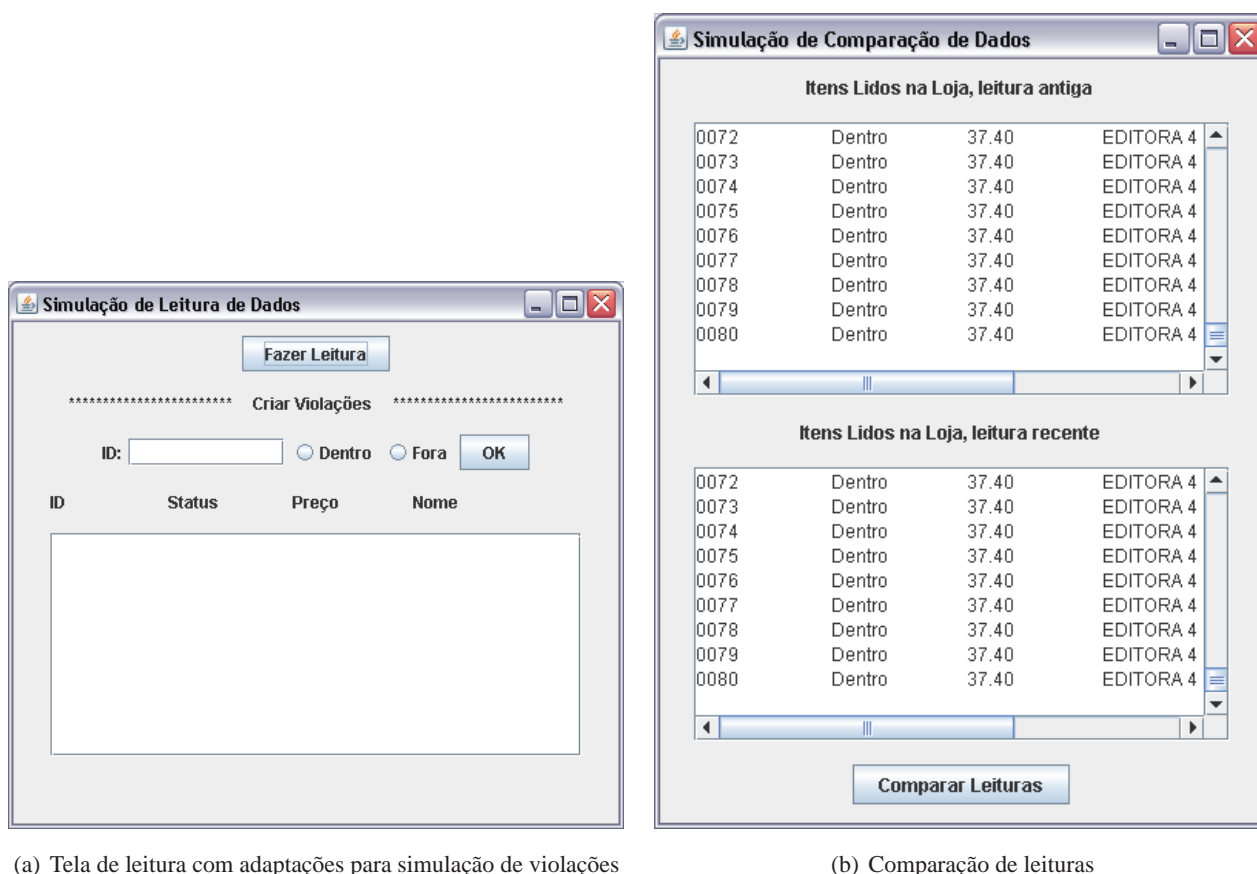
2. Selecionar **Leitura da loja**.

   Esse tópico abre uma janela, figura 5.10 (a). Ao se clicar no botão **Fazer leitura**, o software realiza uma leitura do estoque existente na loja. Caso essa seja a primeira leitura do dia, deve-se fazer uma nova leitura, selecionando-se novamente **Leitura da loja**. Caso já exista uma leitura anterior, não é necessário solicitar essa leitura. Se não houverem duas leituras para comparação, ao tentar realizar a comparação, o sistema emitirá uma mensagem alertando para o número insuficiente de leituras.

   A realização de leituras é simulada no software proposto a partir da cópia da tabela de estoque para a de leitura, o que corresponde à identificação de todos os itens existentes em estoque.

3. Para simular possíveis violações, o campo **Criar Violações** da tela ilustrada na figura 5.10 (a), permite que dados de livros sejam alterados em cada uma das tabelas de leitura, sem modificar os dados originais, na tabela de estoque. Essa adaptação simula violações, já que no intervalo de tempo entre duas leituras houve alteração do status de exemplares (status **dentro** alterado para **fora** ou vice-versa), mas não houve venda desses livros. Depois de realizar as possíveis violações, a janela de

leitura deve ser fechada.

4. Para realizar a comparação entre as leituras, no menu **Sistema RFID**, clica-se em **Compara Leituras**. A janela aberta, ilustrada na figura 5.10 (b), mostra as duas leituras mais recentemente realizadas, com os itens que marcados com o status dentro (supostamente em estoque) em cada uma delas. Os itens que constarem em uma tabela e não constarem na outra (conflitos), independente da seqüência de leitura, são confrontados com aqueles existentes na tabela de vendas. Caso não constem nessa tabela, necessariamente foram furtados ou violados, e o sistema dispara uma mensagem de alerta.

(a) Tela de leitura com adaptações para simulação de violações

(b) Comparação de leituras

Figura 5.10: Simulação do software embarcado nos leitores

5.9 CONSOLIDAÇÃO DE DADOS

As informações de cadastro são armazenadas no banco de dados MySQL, instalado com o software. Esse banco de dados não é de fácil acesso para o usuário, além de conter todas as informações do software. Para maior segurança dos dados e consulta das informações cadastradas, o software oferece opção de geração de relatórios e estatísticas a partir do menu ilustrado na figura I.11 (a).

Ao clicar em **Relatórios**, a janela da figura I.11 (b) é mostrada, com as opções de formatação do relatório a ser obtido. É possível escolher o tipo de relatório: estoque, vendas ou violações; tipo de filtro: sem filtro (mostra todos os registros do sistema), autor, nome do livro, editora, preço ou data; tipo de ordenação: por autor, nome do livro, editora ou ID. Os campos **Valor inicial** e **Valor final** permitem

escolher a faixa de preço para o filtro; os campos **Data inicial** e **Data final** determinam o intervalo de tempo para o filtro de data e o campo **Autor/Editora/Livro** é um campo livre, que permite filtragem dos dados que se iniciam com o texto inserido. Os relatórios emitidos são salvos no diretório C: do computador, denominados pelo tipo do filtro utilizado e data de emissão.

Se o campo **Estatísticas** for selecionado, na janela que se abre, ilustrada na figura I.11 (b), é possível determinar um prazo e verificar, dentro desse período, estatísticas referentes aos dados do sistema.

Se o usuário clicar no botão **Estoque**, na tela são apresentadas quantidade de produtos estocados, valor acumulado desses itens, o livro em maior quantidade em estoque, aquele em menor quantidade e o mais antigo em estoque. Todos os campos referenciados ao período selecionado.

Se o botão **Venda** for selecionado, são apresentados a quantidade dos itens vendidos, valor dos livros vendidos, o lucro obtido e o item mais vendido, também relativos ao período em questão.

Se pressionar o botão **Violações**, são apresentados, para o período em questão, a quantidade de produtos violados, o valor dos livros violados, o item mais furtado e a quantidade de furtos desse item.

Ao selecionar **Calcula lucro**, são apresentados as quantidades dos produtos mais vendidos, o valor de compra e o valor de venda total dos produtos, o lucro real e o percentual obtido no período delimitado.

5.10 ESTUDO DE CASO

Para exemplificar a utilização do software, considere o cadastro das editoras e livros especificados a seguir. O funcionamento de todo o software será ilustrado a partir desses cadastros. Os dados de editoras para cadastro são mostrados na tabela 5.1. Os dados dos livros da editora Saraiva estão na tabela 5.2 e os da editora Método, na tabela 5.3.

Tabela 5.1: Editoras para cadastro.

Nome	Editora Saraiva	Editora Método
Endereço	Av. Marquês de São Vicente, 1967	R. Conselheiro Ramalho, 692/694
	Barra Funda, São Paulo-SP	Bela Vista, São Paulo-SP
Contato	João da Silva	Maria do Carmo
e-mail	saraivajur@editorasaraiva.com.br	metodo@editorametodo.com.br
Telefone	(11)3613 3344	(11)3215 8350

Os passos do cadastro desses itens serão mostrados a seguir, como exemplo de aplicação do software. O exemplo é para o software sendo usado pela primeira vez.

1. Acesso

   Na tela de permissão de acesso, o administrador do software utiliza o usuário **MASTER** e a senha **1234**, como ilustrado na figura 5.12, para acessar o programa.

2. Cadastro de usuários

   No menu **Arquivo**, seleciona **Cadastrar Usuário**. Na tela que se abre, são cadastrados três usuários, com acessos somente às suas respectivas áreas:

(a) Menu relatórios e estatísticas.

(b) Tela de relatórios.

(c) Tela de estatísticas.

Figura 5.11: Utilitários de consolidação de informações

- Usuário 1 - Acesso aos cadastros de editoras e livros;
- Usuário 2 - Acesso ao estoque para consulta e cadastro;
- Usuário 3 - Acesso a vendas.

A figura 5.13 mostra tais opções de cadastro.

3. Cadastro das editoras

   O usuário 1 é o primeiro a utilizar o sistema, com o seu acesso às telas de cadastro. Os dados de cadastro das editoras indicados na tabela 5.1 devem ser preenchidos como na figura 5.14. O mesmo

Tabela 5.2: Livros da Editora Saraiva para cadastro.

Nome	Direito Eleitoral	Direito do Trabalho
Autor	Celso Spitzcovsky	Carlos Roberto Gonçalves
Edição	2007	2006
Páginas	280	200
ISBN	85-02-05664-6	85-02-05874-6
Preço	23.92	20.57
Margem de Lucro	20%	20%
Quantidade	30	20

Tabela 5.3: Livros da Editora Método para cadastro.

Nome	Direito do Trabalho para Concursos Públicos
Autor	Renato Saraiva
Edição	2007
Páginas	468
ISBN	978-85-7660-182-1
Preço	60.00
Margem de Lucro	40%
Quantidade	50

procedimento é seguido para cadastro da Editora Método. Para visualizar os dados das editoras já cadastradas, utiliza-se a consulta, como ilustrado na figura 5.15.

4. Cadastro de livros

   O mesmo usuário deve cadastrar os livros indicados pela tabela 5.2. Como a editora já foi cadastrada, no campo editora a opção **Saraiva** já aparece. É interessante ressaltar que mesmo sendo dois livros distintos, não é necessário cadastrar a editora duas vezes. A figura 5.16 (a) ilustra o cadastro de um livro: depois de preencher todos os dados, clica-se em cadastrar. Para cadastro dos demais, repete-se o procedimento. Caso deseje-se alterar o preço de um produto, a margem de lucro ou excluí-lo do sistema, é possível a partir da identificação do nome do livro na parte de **Fazer Consultas e Alterações**, figura 5.16 (b). O novo preço de compra ou a margem de lucro são preenchidos e inseridos no banco de dados pelo botão **Alterar**. A exclusão do item é feita pelo botão **Apagar Produto**. Para sair do software, o usuário deve seguir por **Arquivo>Sair**.

5. Cadastro em estoque

   As quantidades de cada exemplar mostradas nas tabelas 5.2 e 5.3 devem ser cadastradas pelo usuário 2, que possui a permissão para esse acesso. O software automaticamente cria uma identificação seqüencial para as novas entradas, baseada na identificação do último exemplar cadastrado. A figura 5.17 (a) ilustra o cadastro em estoque de um item. Para sair do software, o usuário deve seguir por **Arquivo>Sair**.

6. Vendas

Figura 5.12: Primeiro acesso ao sistema com o usuário master.

(a) Usuário 1. (b) Usuário 2. (c) Usuário 3.

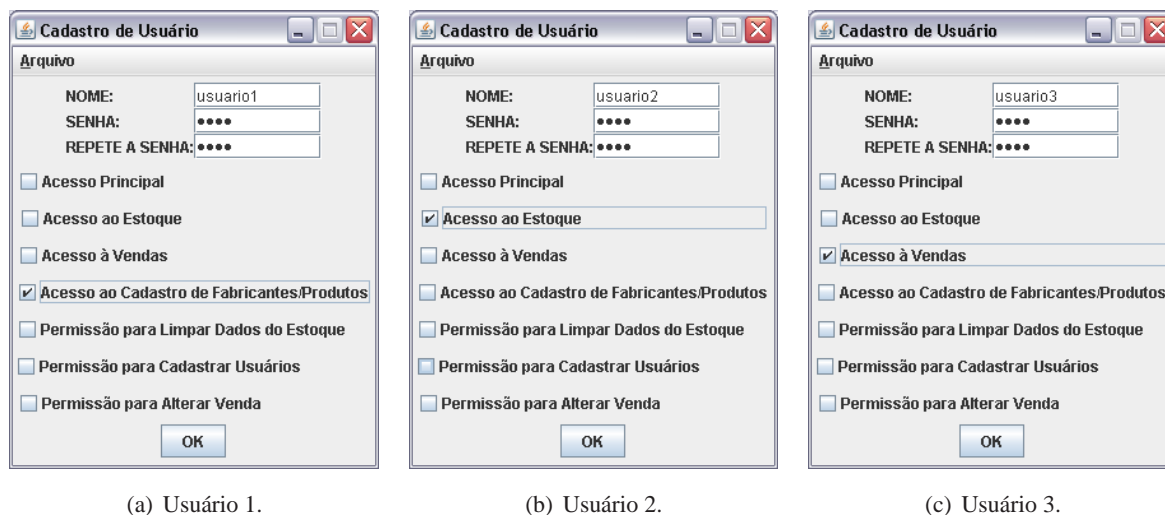



Figura 5.13: Cadastro dos usuários com permissões limitadas.

O usuário 3 é o responsável por vendas. Ele deve registrar os produtos escolhidos pelos clientes, clicando em **Vender** e receber o valor final da venda e só então pressionar em **Finalizar Venda**, figura 5.17 (b). Caso algum item seja registrado como vendido incorretamente, somente o usuário responsável pela exclusão da venda pode realizar tal operação. Ele deve apertar o botão **Excluir Item** e inserir o nome e a senha de usuário na tela de permissão. Para sair do software, o usuário deve seguir por **Arquivo>Sair**.

7. Sistema RFID

   Para testar o sistema RFID adaptado no software, uma leitura inicial é feita por qualquer um dos usuários. Para isso, seleciona-se **Sistema RFID** no menu principal, **Leitura da Loja** e na janela de simulação de leitura, pressiona-se o botão **Fazer Leitura** e então fecha-se a janela pelo botão X na barra superior direita.

   Uma nova leitura é feita para simulação de violações, ilustrada na figura 5.18 (a). Os livros 0031, 0032 e 0055 que estão no estoque tiveram seu status alterado para **fora**. Na tela de comparação, figura 5.18 (b), os exemplares violados na segunda leitura não aparecem, pois em um sistema real itens violados não são lidos. As diferenças entre as duas leituras são identificadas pelo sistema como conflito e comparadas à tabela de vendas. Como nenhum desses itens foi vendido, o sistema os identifica como violações e dispara um alerta de violação, figura 5.18 (c).

8. Emissão dos relatórios

   Para melhor visualização do banco de dados, o sistema oferece a opção de emissão de relatórios,

Figura 5.14: Cadastro de Editora.

através no menu principal. Seleciona-se **Relatórios e Estatísticas** e então clica-se em **Relatórios**. Para emissão de um relatório de estoque com todos os itens existentes na loja, deve-se escolher na opção **Tipo de Filtro: Nenhum Filtro**, para que todos os itens sejam mostrados. A ordenação depende da preferência do usuário ou da aplicação do relatório. A figura 5.19 (a) ilustra a solicitação desse tipo de relatório, ordenado por Editora. A figura 5.19 (c) mostra o resultado obtido do relatório, salvo no diretório C: do computador. O nome do documento referencia o dia de emissão do relatório.

Para emissão de um relatório de vendas, é necessário solicitar o **Tipo de Relatório: Vendas**, **Tipo de filtro:** pode ser por **Nome do Livro**, o que habilita o campo **Autor/Editora/Livro**, figura 5.19 (b). Esse campo pode ser preenchido com o começo da palavra que se deseja filtrar. Por exemplo, solicitou-se o relatório de vendas dos exemplares que têm nome começado por "Dir". Como todos os exemplares vendidos têm o nome iniciado pelo campo solicitado, todos aparecem no relatório. O campo **Ordenar por: Nome do Livro** indica que o campo nome está em ordem alfabética, como ilustrado na figura 5.19 (d), diferente do relatório de estoque da figura5.19 (c), que foi ordenado por editora.

9. Estatísticas

   Como o cadastro do exemplo foi realizado todo na data 04/12/2007 solicitou-se as estatísticas referentes a essa data. As figuras 5.20 (a), (b), (c), e (d) ilustram as estatísticas dos itens cadastrados, vendidos, violados e o cálculo do lucro da loja.

Figura 5.15: Consulta de Editora

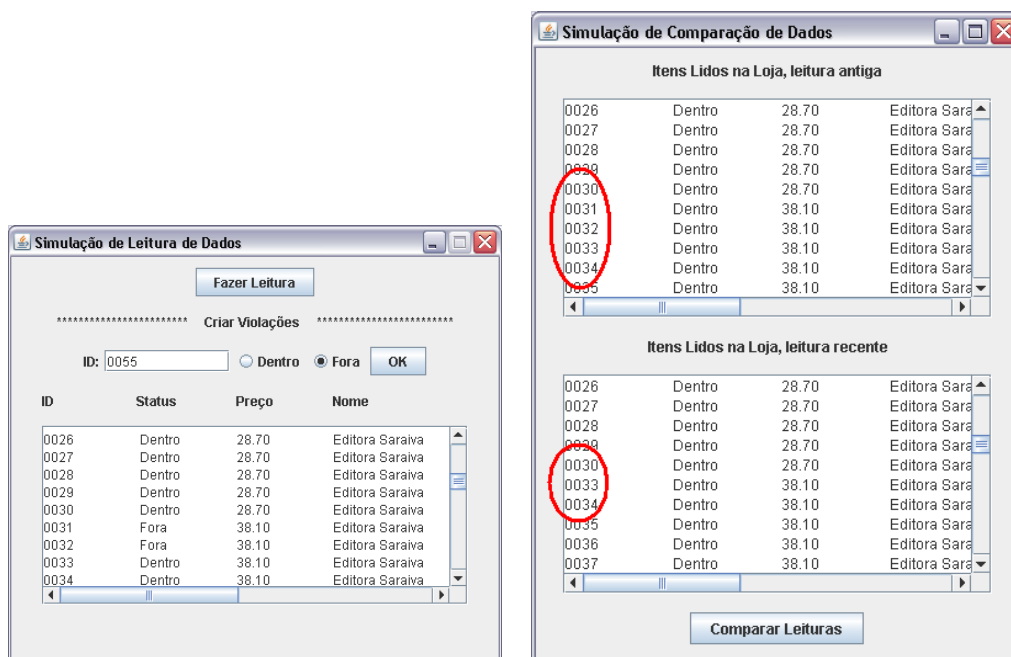
(a) Cadastro de um livro.

(b) Consulta para alteração ou exclusão de um item cadastrado.

Figura 5.16: Cadastro e consulta dos livros.

(a) Cadastro em estoque.

(b) Exemplo de venda de produtos.

Figura 5.17: Cadastro em estoque e vendas.

(a) Simulação de violações dos itens 0031, 0032 e 0055.

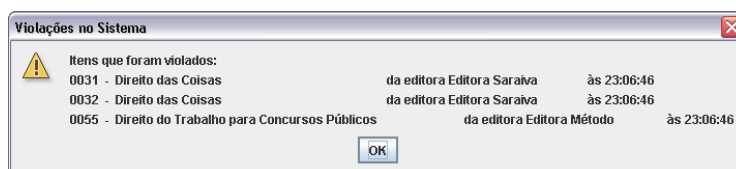
(b) Tela de comparação entre as leituras.

(c) Alerta de violação dos itens indicados.

Figura 5.18: Simulação do sistema RFID.

(a) Solicitação de relatório de estoque. (b) Solicitação de relatório de vendas.

Relatorio de Estoque Filtro Nenhum Filtro dia 2007-12-04.txt - Bloco de notas

Arquivo Editar Formatar Exibir Ajuda

DIA	ID	PREÇO	EDITORA	NOME DO LIVRO	AUTOR
2007-12-04	0051	84.00	Editora Método	Direito do Trabalho para Concursos Públicos	Renato Saraiva
2007-12-04	0052	84.00	Editora Método	Direito do Trabalho para Concursos Públicos	Renato Saraiva
2007-12-04	0053	84.00	Editora Método	Direito do Trabalho para Concursos Públicos	Renato Saraiva
2007-12-04	0054	84.00	Editora Método	Direito do Trabalho para Concursos Públicos	Renato Saraiva
2007-12-04	0055	84.00	Editora Método	Direito do Trabalho para Concursos Públicos	Renato Saraiva
2007-12-04	0056	84.00	Editora Método	Direito do Trabalho para Concursos Públicos	Renato Saraiva
2007-12-04	0057	84.00	Editora Método	Direito do Trabalho para Concursos Públicos	Renato Saraiva
2007-12-04	0058	84.00	Editora Método	Direito do Trabalho para Concursos Públicos	Renato Saraiva
2007-12-04	0059	84.00	Editora Método	Direito do Trabalho para Concursos Públicos	Renato Saraiva
2007-12-04	0060	84.00	Editora Método	Direito do Trabalho para Concursos Públicos	Renato Saraiva
2007-12-04	0061	84.00	Editora Método	Direito do Trabalho para Concursos Públicos	Renato Saraiva
2007-12-04	0062	84.00	Editora Método	Direito do Trabalho para Concursos Públicos	Renato Saraiva
2007-12-04	0063	84.00	Editora Método	Direito do Trabalho para Concursos Públicos	Renato Saraiva
2007-12-04	0064	84.00	Editora Método	Direito do Trabalho para Concursos Públicos	Renato Saraiva
2007-12-04	0065	84.00	Editora Método	Direito do Trabalho para Concursos Públicos	Renato Saraiva
2007-12-04	0066	84.00	Editora Método	Direito do Trabalho para Concursos Públicos	Renato Saraiva
2007-12-04	0067	84.00	Editora Método	Direito do Trabalho para Concursos Públicos	Renato Saraiva
2007-12-04	0068	84.00	Editora Método	Direito do Trabalho para Concursos Públicos	Renato Saraiva
2007-12-04	0069	84.00	Editora Método	Direito do Trabalho para Concursos Públicos	Renato Saraiva
2007-12-04	0070	84.00	Editora Método	Direito do Trabalho para Concursos Públicos	Renato Saraiva
2007-12-04	0071	84.00	Editora Método	Direito do Trabalho para Concursos Públicos	Renato Saraiva
2007-12-04	0072	84.00	Editora Método	Direito do Trabalho para Concursos Públicos	Renato Saraiva
2007-12-04	0073	84.00	Editora Método	Direito do Trabalho para Concursos Públicos	Renato Saraiva
2007-12-04	0074	84.00	Editora Método	Direito do Trabalho para Concursos Públicos	Renato Saraiva
2007-12-04	0075	84.00	Editora Método	Direito do Trabalho para Concursos Públicos	Renato Saraiva
2007-12-04	0076	84.00	Editora Método	Direito do Trabalho para Concursos Públicos	Renato Saraiva
2007-12-04	0077	84.00	Editora Método	Direito do Trabalho para Concursos Públicos	Renato Saraiva
2007-12-04	0078	84.00	Editora Método	Direito do Trabalho para Concursos Públicos	Renato Saraiva
2007-12-04	0079	84.00	Editora Método	Direito do Trabalho para Concursos Públicos	Renato Saraiva
2007-12-04	0080	84.00	Editora Método	Direito do Trabalho para Concursos Públicos	Renato Saraiva
2007-12-04	0081	84.00	Editora Método	Direito do Trabalho para Concursos Públicos	Renato Saraiva
2007-12-04	0082	84.00	Editora Método	Direito do Trabalho para Concursos Públicos	Renato Saraiva
2007-12-04	0083	84.00	Editora Método	Direito do Trabalho para Concursos Públicos	Renato Saraiva
2007-12-04	0084	84.00	Editora Método	Direito do Trabalho para Concursos Públicos	Renato Saraiva
2007-12-04	0085	84.00	Editora Método	Direito do Trabalho para Concursos Públicos	Renato Saraiva
2007-12-04	0086	84.00	Editora Método	Direito do Trabalho para Concursos Públicos	Renato Saraiva
2007-12-04	0087	84.00	Editora Método	Direito do Trabalho para Concursos Públicos	Renato Saraiva
2007-12-04	0088	84.00	Editora Método	Direito do Trabalho para Concursos Públicos	Renato Saraiva
2007-12-04	0089	84.00	Editora Método	Direito do Trabalho para Concursos Públicos	Renato Saraiva
2007-12-04	0090	84.00	Editora Método	Direito do Trabalho para Concursos Públicos	Renato Saraiva
2007-12-04	0091	84.00	Editora Método	Direito do Trabalho para Concursos Públicos	Renato Saraiva
2007-12-04	0092	84.00	Editora Método	Direito do Trabalho para Concursos Públicos	Renato Saraiva
2007-12-04	0093	84.00	Editora Método	Direito do Trabalho para Concursos Públicos	Renato Saraiva

(c) Relatório de estoque emitido.

Relatorio de Vendas Filtro Produto dia 2007-12-04.txt - Bloco de notas

Arquivo Editar Formatar Exibir Ajuda

DIA	ID	PREÇO	EDITORA	NOME DO LIVRO	AUTOR
2007-12-04	0043	38.10	Editora Saraiva	Direito das Coisas	Carlos Roberto Gonçalves
2007-12-04	0063	84.00	Editora Método	Direito do Trabalho para Concursos Públicos	Renato Saraiva
2007-12-04	0078	84.00	Editora Método	Direito do Trabalho para Concursos Públicos	Renato Saraiva
2007-12-04	0002	28.70	Editora Saraiva	Direito Eleitoral	Celso Spitzcovsky

(d) Relatório de vendas emitido.

Figura 5.19: Relatórios.

(a) Estatísticas de estoque.

(b) Estatísticas de vendas.

(c) Estatísticas de violações.

(d) Cálculo de lucro da loja no período.

Figura 5.20: Estatísticas

6 CONCLUSÃO

O mundo tecnológico hoje está se desenvolvendo significativamente na área de transmissão de dados sem fio e com segurança. Nesse contexto, o RFID é uma solução que se destaca, por custo relativamente baixo, por permitir trocas de dados em curtas distâncias com velocidade na transação, segurança de produtos e pessoas.

As aplicações para essa tecnologia são incontáveis. Pode-se citar desde aplicações de melhoria de qualidade de vida, como tags com informações hospitalares de cada paciente, o que evita erros de diagnósticos, repetições de exames e até mesmo acelera o processo de atendimento, que em alguns casos, pode significar salvar vidas. Existem aplicações mais funcionais, como dados pessoais armazenados em um cartão contendo uma tag RFID, como uma identidade digital, que dispensaria a necessidade de carregar diversos documentos e cartões. Ao solicitar emissão de mais um documento, o cidadão deveria apenas atualizar os dados da tag em postos indicados, o que diminuiria as filas de emissão de documentos, segunda via e seria uma melhoria dos serviços prestados pelo governo.

Essas aplicações envolvem privacidade e segurança da população. A resistência em adotá-las e até mesmo testá-las é grande. Se por um lado existem muitos benefícios, por outro lado, caso a segurança não seja fortemente projetada, há o risco de transtornos que podem trazer danos irreversíveis. Um exemplo é o risco de confiar em dados hospitalares armazenados em chips que, em situação de emergência, podem não fornecer os dados com o histórico do paciente ou corromper os dados. Nesses casos, onde há risco de vida, a mudança dos tradicionais prontuários à mão para inovações tecnológicas demanda um estudo minucioso de segurança de informação e confiabilidade da tecnologia. Esses impecílios levaram ao desenvolvimento dessa tecnologia mais voltado para o comércio.

A facilidade de rastreabilidade das etiquetas RFID trouxe um grande desenvolvimento na área controle de produtos e inventário. É possível facilmente controlar uma produção completa e as unidades fabris utilizando tecnologia RFID. Grandes lojas de departamento já empregam esse sistema, para segurança de seus produtos, mas sem utilizar etiquetas com capacidade de armazenamento de dados. Qualquer tipo de estabelecimento comercial, no entanto, tem necessidade de controlar entrada e saída da loja, para garantir segurança. O RFID traz uma comodidade nesse sentido, pois torna possível o controle dos produtos a todo momento e dispensa a necessidade de dedicação exclusiva de funcionários para controle de estoque e fiscalização de saída de produtos. Um computador ligado a um ou mais leitores é capaz de verificar periodicamente a segurança dos itens em estoque, aumentando as chances de flagrar uma tentativa de furto no momento da infração.

A tecnologia RFID só tem utilidade se seus dados forem tratados corretamente por um sistema computacional. A aquisição dos dados por si só é inútil, pois é essencial a interpretação dos mesmos. O sistema acoplado auxilia e integra as etapas da tecnologia, fazendo com que os dados deixem de ser apenas um conjunto de informações ilegíveis e passem a ser ferramentas de segurança. A utilização de soluções pré-formatadas, no entanto, agrega valor ao sistema RFID completo e dificulta o acesso aos pequenos investidores, devido ao custo elevado. Neste trabalho, foram estudadas duas iniciativas de grandes fabricantes: Solução IBM e Savant Concentrator; e foi proposta uma versão inicial de uma das ferramentas

necessárias para a implantação de um sistema RFID.

A solução IBM, quando comparada às outras em questão, é a mais completa. Possui uma divisão bem estudada de atividades realizadas e garante para o cliente uma solução fim a fim. Implanta desde a captura de dados das etiquetas até as decisões tomadas para garantia de segurança, como disparo de sirenes ou alarmes, fechamento de portas, ou mesmo acionamento de seguranças ou policiais. Permite que o cliente configure as ferramentas padrão do sistema, utilizadas em diversos tipos de aplicações. Também pode ter funcionalidades extras, voltadas para aplicação específica de interesse do cliente, o que otimiza o sistema. A própria solução também dedica parte de suas funções para integração com a empresa, ou seja, permite aproveitamento de procedimentos, o que evita a necessidade de novos investimentos em treinamento de funcionários ou grandes alterações nas atividades que eles rotineiramente realizam. O mesmo sistema se adequa a várias aplicações, demandando apenas exclusividade no ato de integrar com a empresa. A maior desvantagem dessa solução é a sua complexidade, que exige alto custo. O investimento tão alto em um sistema de segurança acaba sendo vantajoso somente para grandes empresas, que podem diluir os custos na produção em larga escala, mas que podem sofrer furtos mais facilmente em caso de falta de fiscalização.

O Auto-ID Center é um centro de pesquisas tecnológicas voltado para desenvolvimento de tecnologias Auto-ID, como Biometria, Smart Cards e RFID. Um de seus laboratórios, localizado no MIT (Massachussets Institute of Technology), desenvolveu o Savant Concentrator, uma ferramenta necessária para implementação RFID. Esse laboratório é patrocinado por algumas empresas interessadas em utilizar a tecnologia RFID. O desenvolvimento tem por objetivo explorar ao máximo a potencialidade da tecnologia RFID dentro do espaço de aplicações dos investidores. O software é necessário na implementação de um sistema RFID, pois atua como um concentrador de dados, ou seja, realiza interpretações e filtragens à medida que as informações são adquiridas. Com isso, reduz o fluxo de informações pela rede, evitando a sobrecarga. Ele realiza a integração com o sistema de leitores e com o sistema do usuário, mas somente para verificação das melhorias alcançadas em cada novo teste. O Savant é uma ferramenta que faz parte de um estudo tecnológico. O objetivo do Auto-ID center, ao contrário da IBM, não é vender a solução completa para empresas, mas sim desenvolver continuamente a tecnologia para clientes específicos, os investidores. Por isso esse software não apresenta a mesma versatilidade da Solução IBM, que pode ser utilizada em quase todos os tipos de aplicação. As vantagens desse software são a simplicidade, devido as suas aplicações específicas e a facilidade de modularização e integração com outros sistemas ou com mais Savants, para garantir tratamento de todos os dados adquiridos pelos leitores.

O software proposto é um concentrador de dados para uma aplicação específica: uma livraria. Nele são integradas funcionalidades de rastreamento de itens na loja e também ferramentas de gerenciamento de estoque e venda de produtos. A aquisição de dados em um sistema RFID real é proveniente de leitores RFID. No software são feitas adaptações para simulações das leituras. O processamento dos dados nos leitores, que na prática é feito em softwares embarcados, está integrado à aplicação principal. O controle do fluxo de dados na rede está justamente no momento da entrega dos dados da leitora para a aplicação principal. Devido ao fato de o leitor ter capacidade de processamento, ele realiza a comparação das leituras consecutivas e somente passa para a aplicação principal os dados divergentes entre as leituras. A aplicação principal confrontará as informações conflitantes recebidas com a tabela de venda e verificará qual decisão tomar: caso um item tenha sido violado, o sistema lançará um alerta de segurança informando o nome do produto e a data e hora que ele sofreu tal violação. Uma vantagem do sistema RFID no software proposto é o registro do horário em que as violações ocorrem. Isto é importante para confrontar dados do sistema

RFID com os sistemas de câmera de segurança da loja, por exemplo, conferindo maior robustez ao sistema.

Como sugestão de melhoria, propõe-se a agregação de um maior número de leituras para verificação de violações. Este procedimento, feito tanto na solução IBM como no Savant, previne o alerta de segurança para itens que não foram violados, que somente estavam em uma região de sombra do leitor, erro comum em um sistema real. Os conflitos dessa natureza, aqui denominados de erros de leitura, são armazenados em uma tabela do banco de dados para tratamento em uma versão posterior do software. Sugere-se um sistema com premissas definidas pelo usuário para solução dos conflitos de leitura.

Outra sugestão para melhorar o desempenho do sistema é a realização de todas as comparações e pesquisas por tipos primitivos inteiros, por exemplo, ao invés de comparação por objetos Strings, como foi implementado. O ISBN dos produtos pode ser transformado em inteiro para tal atividade. A demanda de processamento é reduzida tornando o software mais rápido.

Com relação às funcionalidades do software, algumas melhorias são propostas. A possibilidade de editar e/ou excluir perfis de usuários e de editoras é bem funcional. Em uma livraria real, funcionários são contratados e demitidos e editoras de livros podem mudar de endereço, contato ou até mesmo deixar de existir.

O software futuramente poderia suportar funções de impressão, tais como: a impressão das etiquetas RFID no ato em que novos produtos são iseridos no estoque; a impressão de cupons fiscais por impressoras térmicas das vendas para clientes também deve ser realizada, visto que é um recurso necessário em sistema real; a possibilidade de envio dos relatórios para uma impressora seria também uma funcionalidade bastante interessante.

O sistema proposto não é um solução fim a fim, visto que não realiza a parte de aquisição de dados do sistema RFID. Porém, ele já se mostra como um grande passo para a implementação de um sistema RFID completo.

REFERÊNCIAS BIBLIOGRÁFICAS

[1] CARDULLO, M. W. Genesis of the versatile rfid tag. *RFID Journal (www.rfidjournal.com)*, 2002.

[2] THE History of RFID Technology. *RFID Journal (www.rfidjournal.com)*, 2002.

[3] FINKENZELLER, K. *RFID Handbook: fundamentals and applications in contactless smart cards and identification*. [S.l.]: John Wiley & Sons, Ltd., 2003.

[4] CATHERINE, M. Nfc forum announces technology architecture. *RFID Journal (www.rfidjournal.com)*, 2001.

[5] FORUM of Near Field Communication. *www.nfc-forum.org*, Acesso em 08/10/2007.

[6] ALLFLEX - Sistema de Identificação Animal. *http://www.allflex.com.br/informacoes/informacoes.php*, Acesso em 29/11/2007.

[7] RFID. *www.wikipedia.com*, Acesso em 19/06/2007.

[8] BOSS, R. W. Rfid technology for libraries. *ALA - American Library Association*, 2004.

[9] SANTINI, A. G. Rfid - identificação por rádio freqüência. Acesso em 20/06/2007, 2006.

[10] AUTO-ID Center Labs. *www.autoidlabs.org*, Acesso em 08/10/2007.

[11] TECHNOLOGY, I. R. Ibm websphere rfid handbook: A solution guide. *IBM*, 2006.

[12] CLARK, S. et al. Auto-id savant specification 1.0. *AUTO-ID CENTER*, 2003.

[13] PALMER, M. Build an effective rfid architecture. *RFID Journal*, 2001.

[14] PILLA, M. L. *A Microarquitetura picoJava-II*. Tese (Doutorado) — Universidade Federal do Rio Grande do Sul, Novembro, 1999.

[15] JEPSON, B. *Programando Banco de Dados em JAVA*. [S.l.]: Makron Books, 1997.

[16] DEITEL, H. M.; DEITEL, P. J. *JAVA, Como Programar*. [S.l.]: Bookman, 2001.

[17] JAVA Platform, Standard Edition 6 API Specification. *http://java.sun.com/javase/6/docs/api/*, Acesso em 03/12/2007.

[18] GUIA do Usuário Java. *http://www.guj.com.br/*, Acesso em 02/12/2007.

[19] MANUAL de Referência do MySQL. *http://www.mysql.com*, Acesso em 02/12/2007.

[20] JAVAFREE.ORG. *http://www.javafree.org/index.jf*, Acesso em 03/12/2007.

[21] ARTICLE:IMASTERFORUM. *http://forum.imasters.com.br/*, Acesso em 26/11/2007.

I. DIAGRAMAS DE BLOCOS

O presente anexo apresenta o diagrama de blocos das classes do software desenvolvido. A relação entre as classes é mostrada de forma concisa.

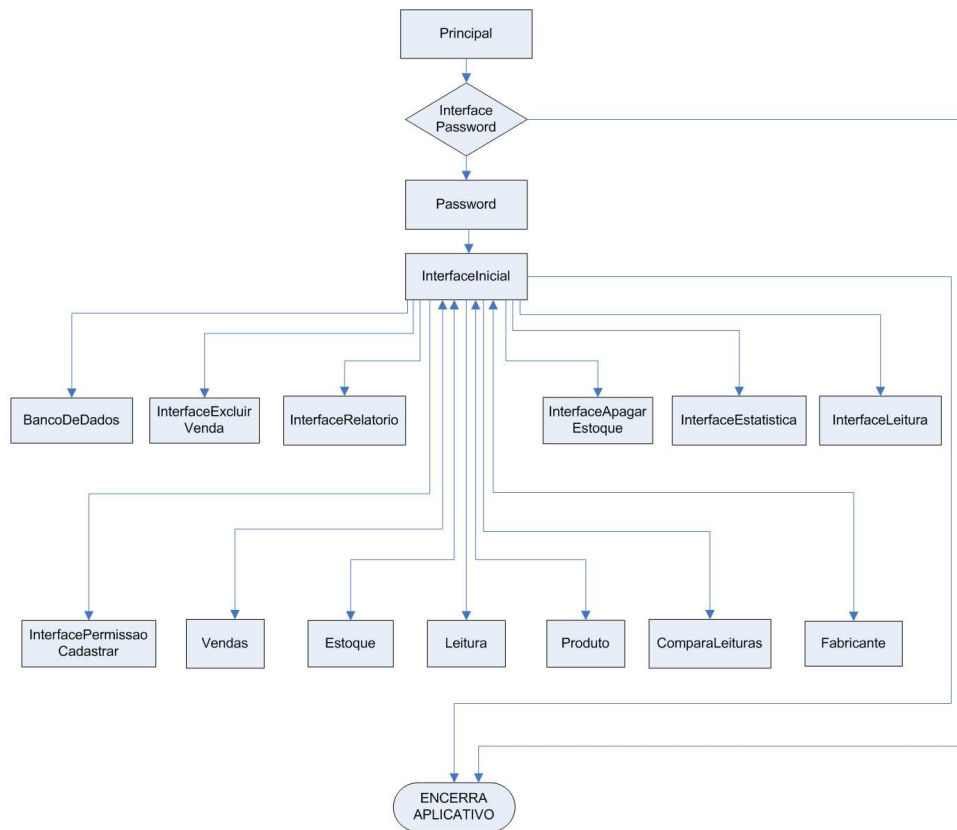



Figura I.1: Diagrama de blocos principal do software.

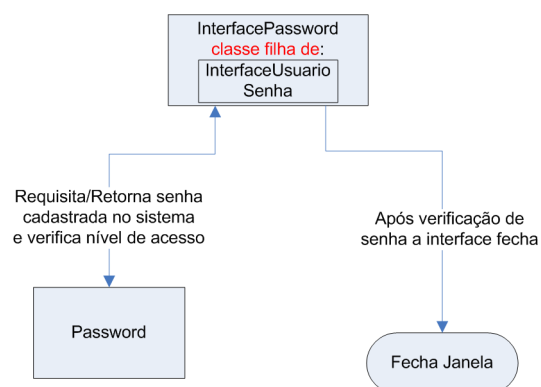



Figura I.2: Diagrama de blocos da classe interface password.

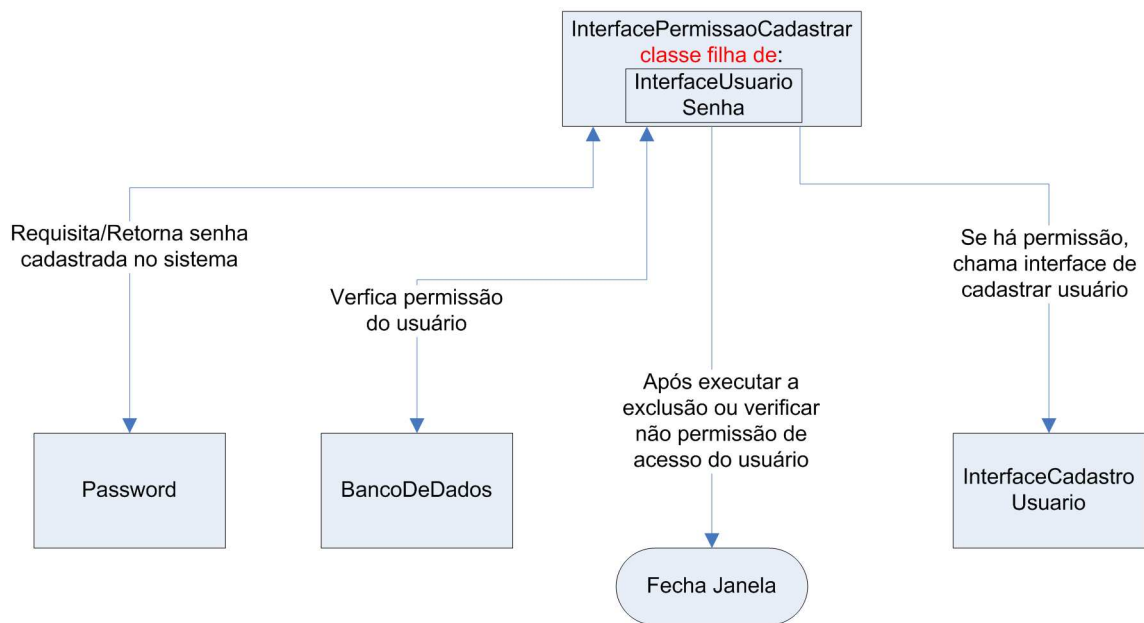



Figura I.3: Diagrama da classe da interface de permissão para cadastro de usuário.

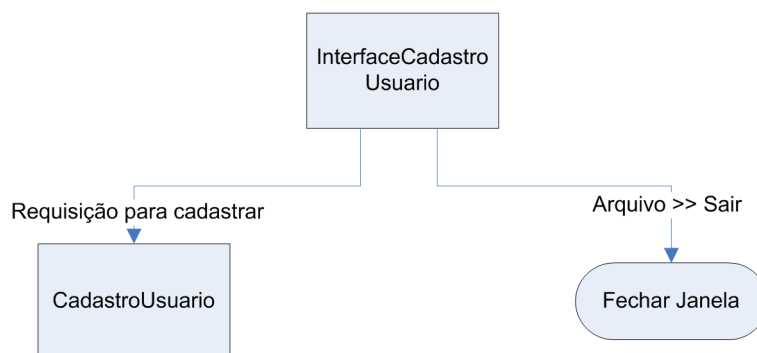



Figura I.4: Diagrama de blocos classe interface de cadastrar usuário.

(a) Classe cadastro usuário. (b) Classe fabricante. (c) Classe produto.

(d) Classe estoque. (e) Classe Vendas. (f) Classe erros violações.

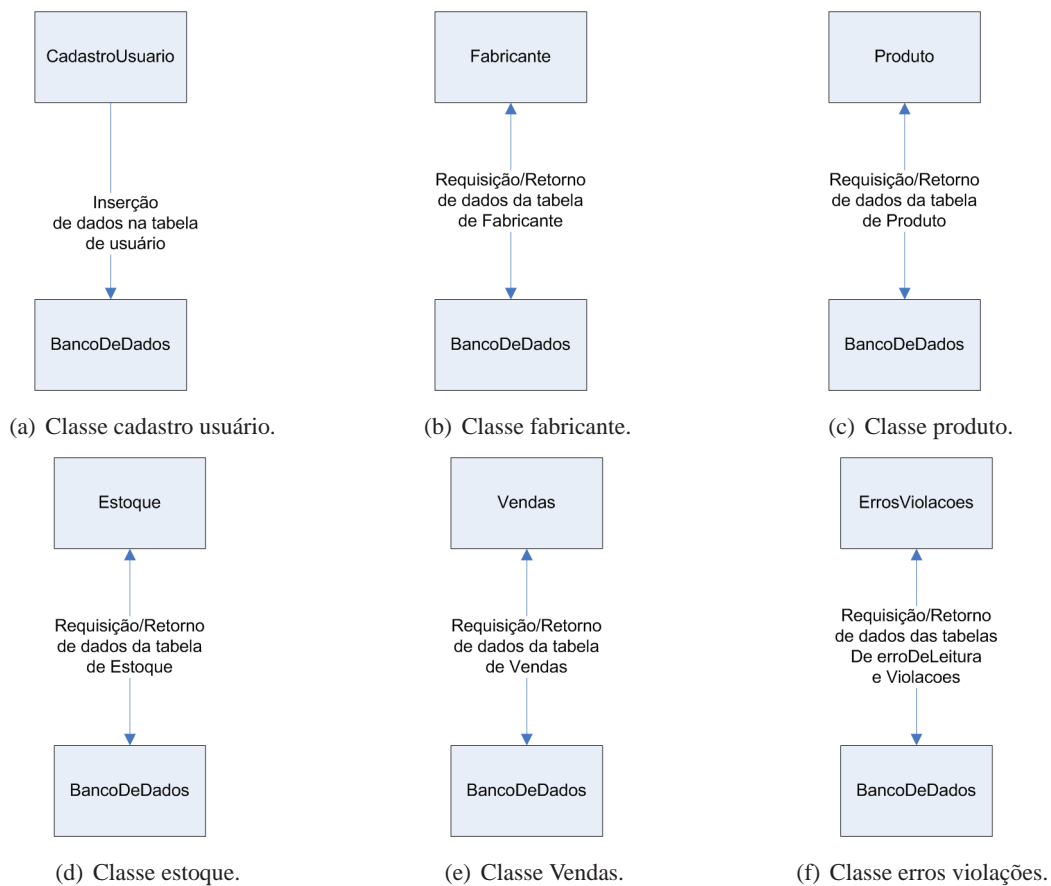



Figura I.5: Diagramas padrão

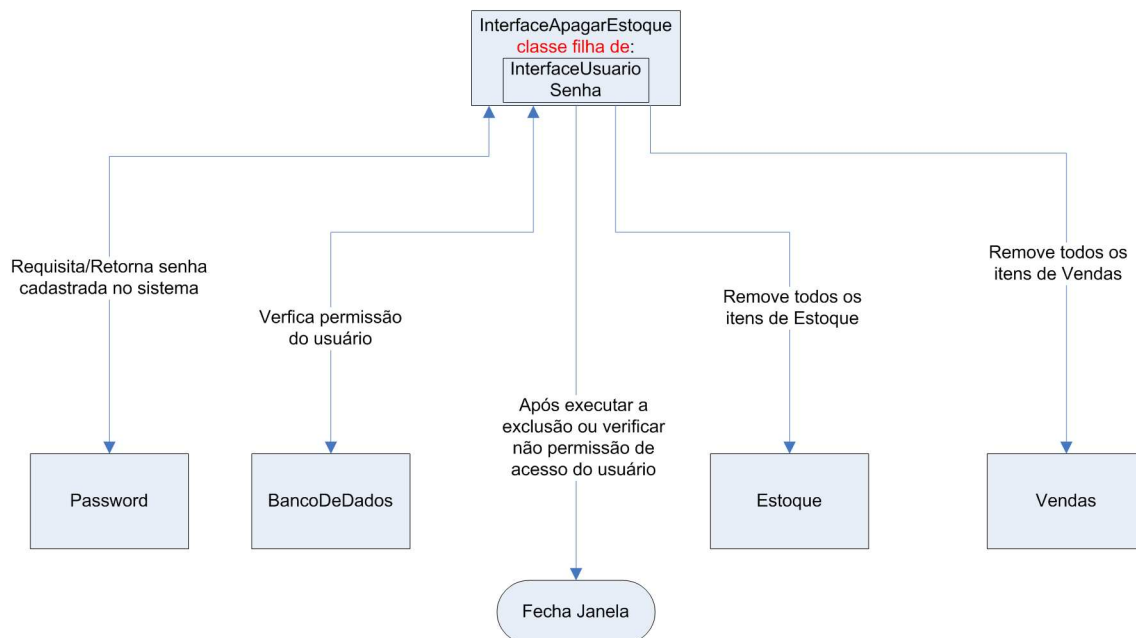



Figura I.6: Diagrama de blocos da classe interface apagar estoque.

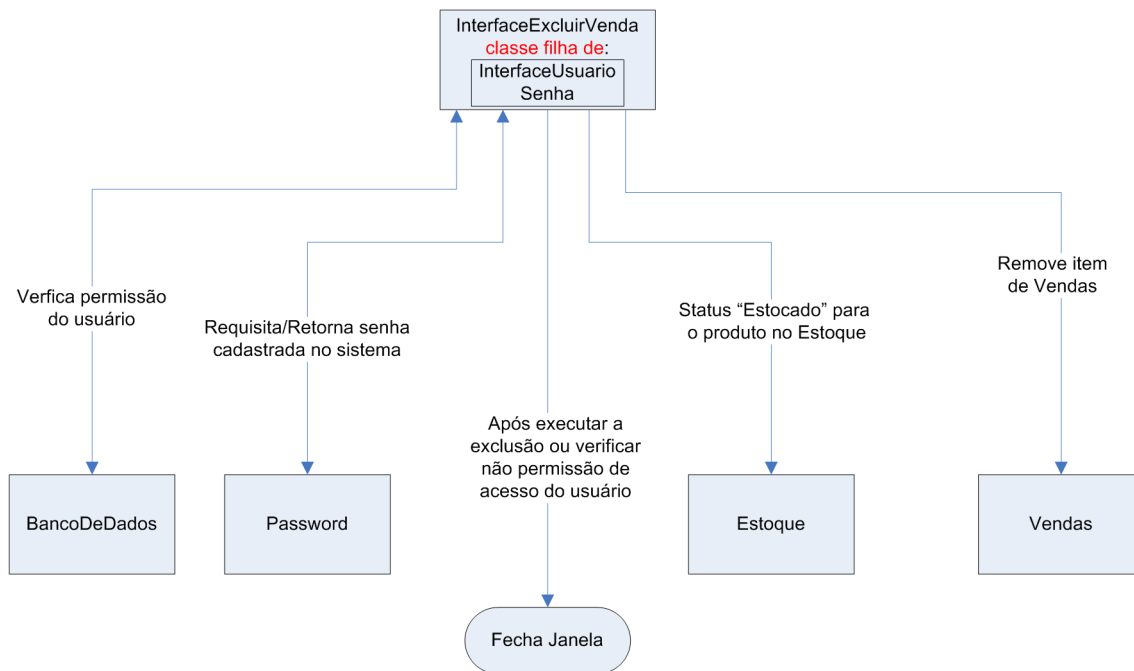



Figura I.7: Diagrama de blocos da classe interface excluir venda.

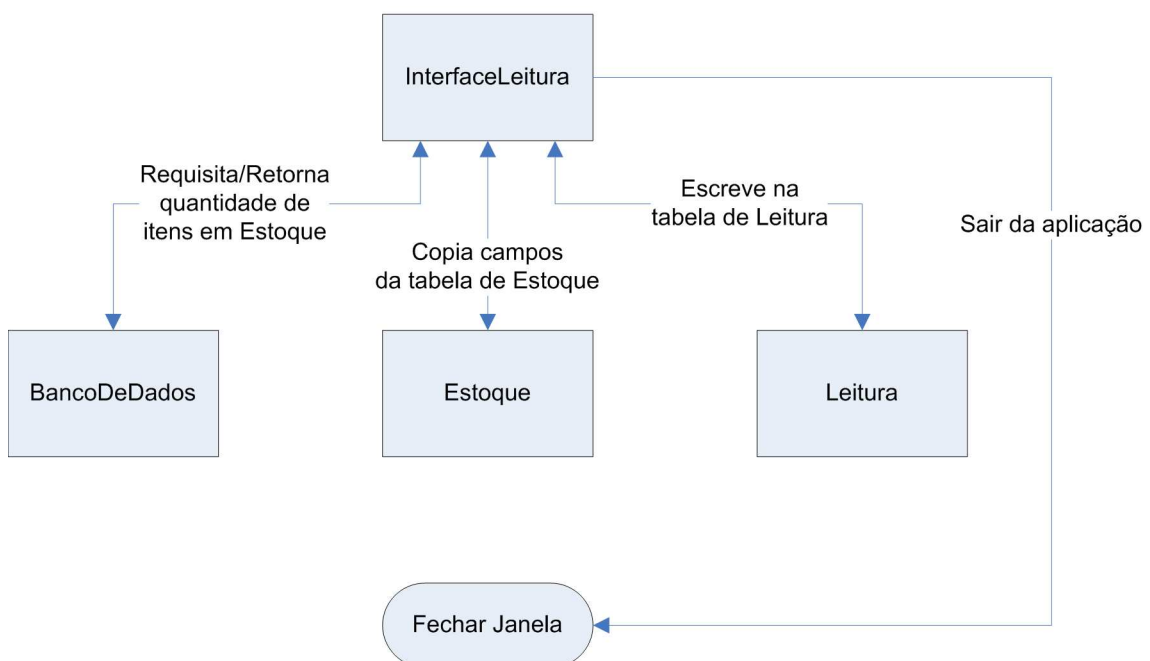



Figura I.8: Diagrama de blocos da classe interface leitura.

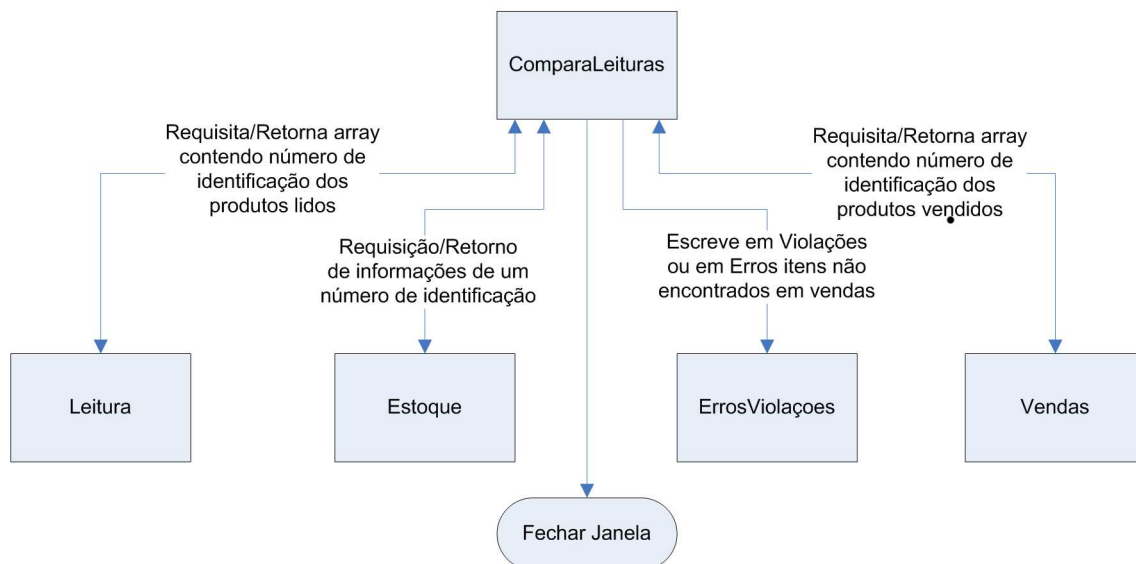



Figura I.9: Diagrama de blocos da classe compara leitura.

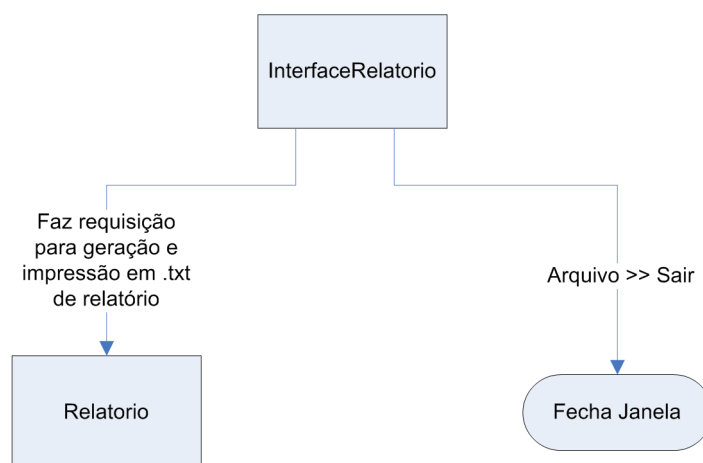



Figura I.10: Diagrama de blocos da classe interface relatório.

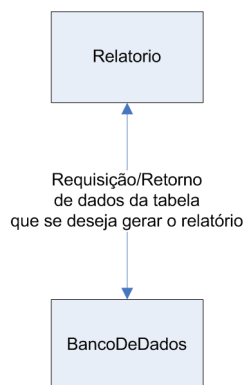



Figura I.11: Diagrama de blocos da classe relatório.

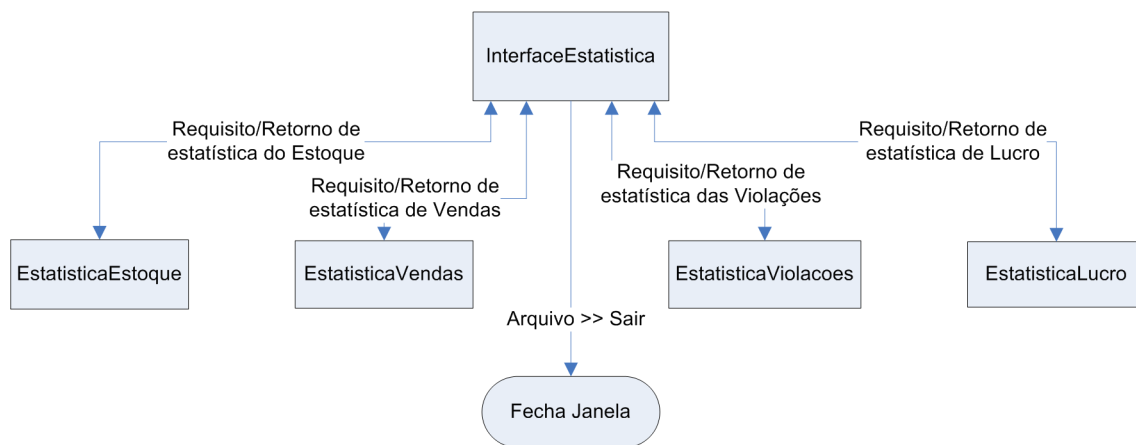



Figura I.12: Diagrama de blocos da classe interface estatística

(a) Classe estatística estoque.

(b) Classe Estatística Vendas.

(c) Classe Estatistica Violações.

(d) Classe Estatística Lucro.

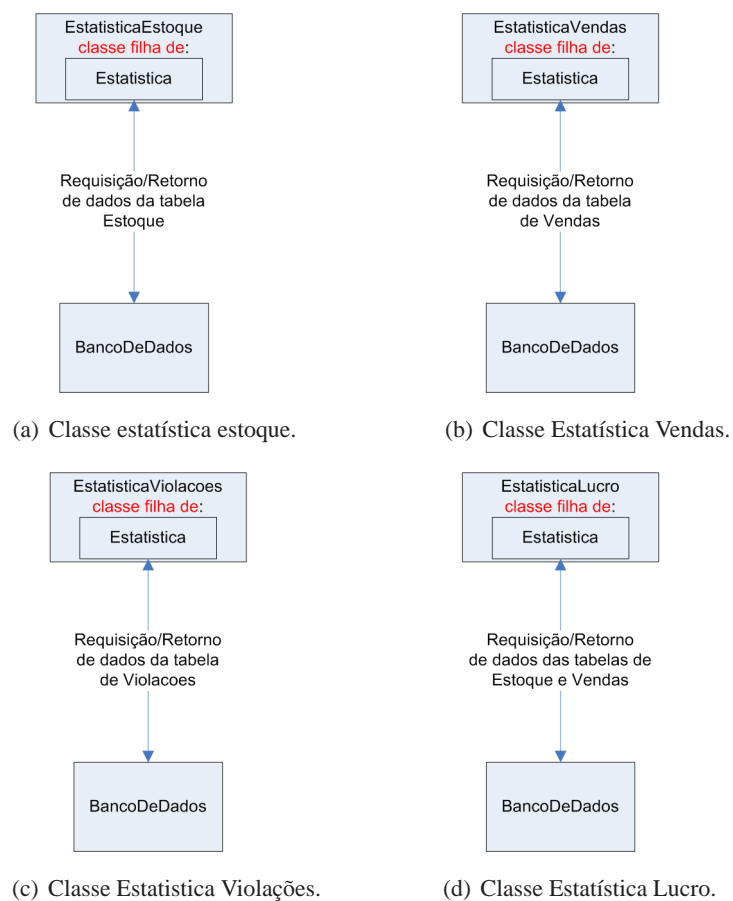



Figura I.13: Diagramas padrão das classes herdadas da classe estatística.

II. DESCRIÇÃO DO CONTEÚDO DO CD

O CD para instalação do software controlador é composto pelos seguintes arquivos:

- MySQL

  Pasta contendo o Setup do MySQL;

- Java

  Pasta contendo o instalador do *Java Runtime Environment* - jre versão 6.3;

- Java-MySQL Conector

  Pasta contendo a pasta com a bilbioteca para comunicação do software com o banco de dados e o instalador para geração do banco de dados e tabelas;

- RFID

  Pasta contendo o software controlador proposto.